Connected Technologies™
A 6110 Lou Street Crystal Lake, IL 60014 | P 815.301.4280 F 815.301.4286 | www.connectedtechnologies.us

Dealer Manual
for

Connect ONE™

Web-Hosted Security & Energy Management

©2014 Connected Technologies, LLC.

Connected Technologies
A 6110 Lou Street Crystal Lake, IL 60014 | P 815.301.4280 F 815.301.4286 | www.connectedtechnologies.us

Table of Contents

Customer Overview 2

New Customer Setup 3

Create a DMP System 5

XR100/500 Communication Setup (V.205 or greater recommended) 8
XR150/350/550 Communication Setup (All versions) 8
XT30/50/XTL Communication Setup (V.103 or greater recommended) 9
Advanced Access Control with DMP 15

Create an ELK System 17

Program the Control Panel 20

Create a Proliphix System 28

Create a Risco System 33

ProSYS Communication Setup 35

Create a Network Gateway System 40

1-Wire Temperature Sensor Wiring Diagram (No Alarm Panel) 48
1-Wire Temperature Sensor Wiring Diagram (CS Alarm Hookup) 49
1-Wire Temperature Sensor Wiring Diagram (Local Alarm Hookup) 50
RCS Thermostats Wiring Diagram 51

Create an Exacq / Ganz / Geovision System 52

Create a Generic IP Camera/DVR System 56

Live Video - IT Instructions 59

How to Setup an Action Rule for Notifications 60

Code Import Utility 63

Customer Overview

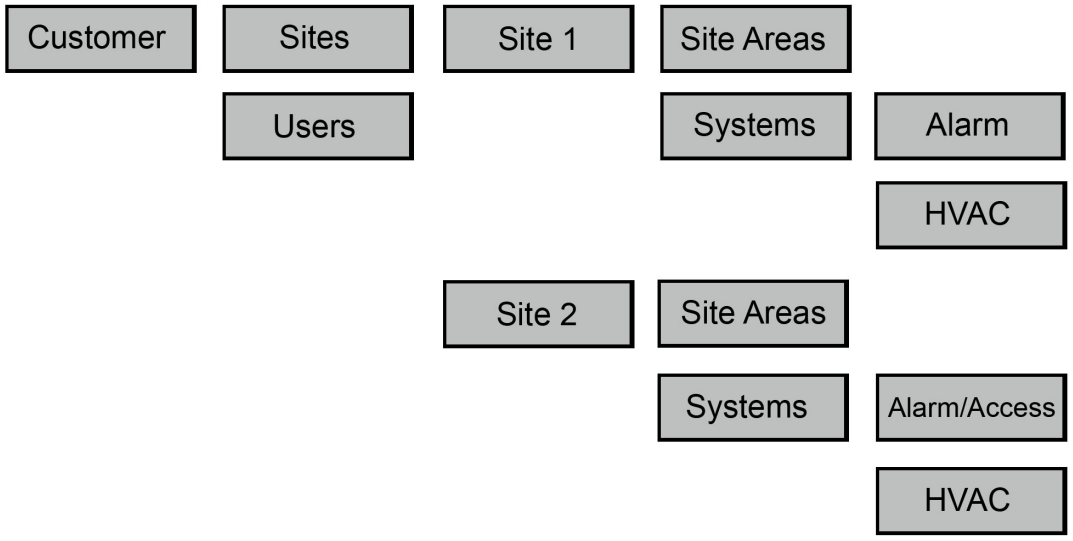


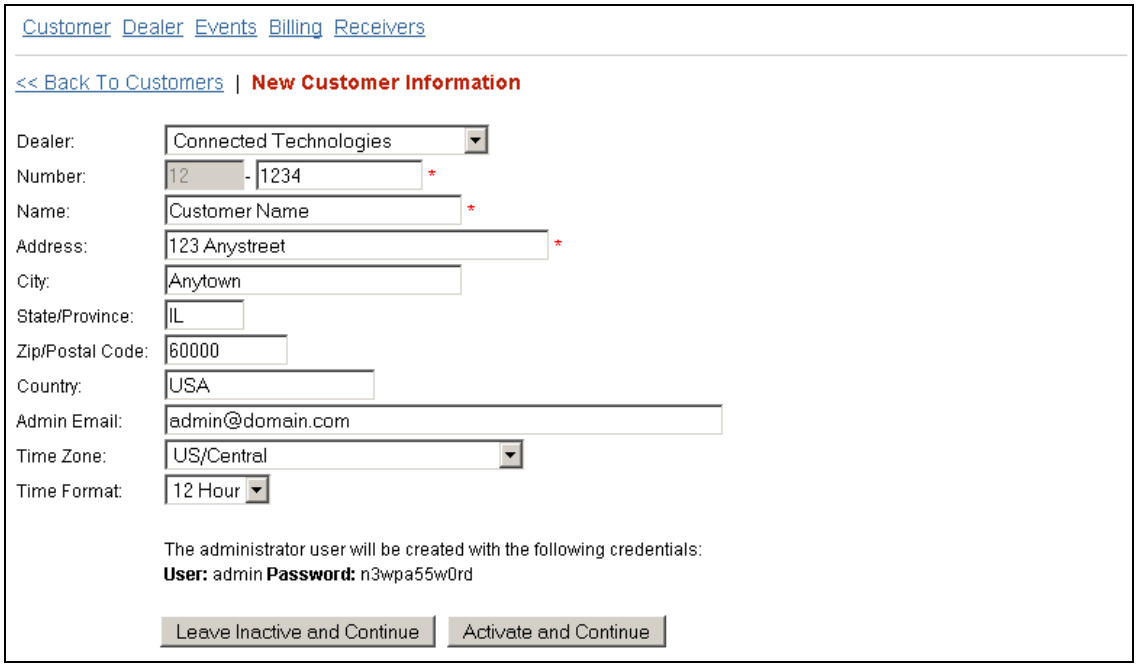
Figure 1: Customer Hierarchy Structure

- The top-most level is the Customer. Below the customer are Sites, Systems and Devices.
- A site is referred to a postal address or single building.
- A system is a grouping of devices.
- A device is referred to a device or control panel. Ex) DMP panel or thermostat.
- The site areas listed under the site are configured in the Connect ONE dealer portal.
- The users under the customer may have access to any number of sites and systems configured for the customer.

Connected Technologies
A 6110 Lou Street Crystal Lake, IL 60014 | P 815.301.4280 F 815.301.4286 | www.connectedtechnologies.us

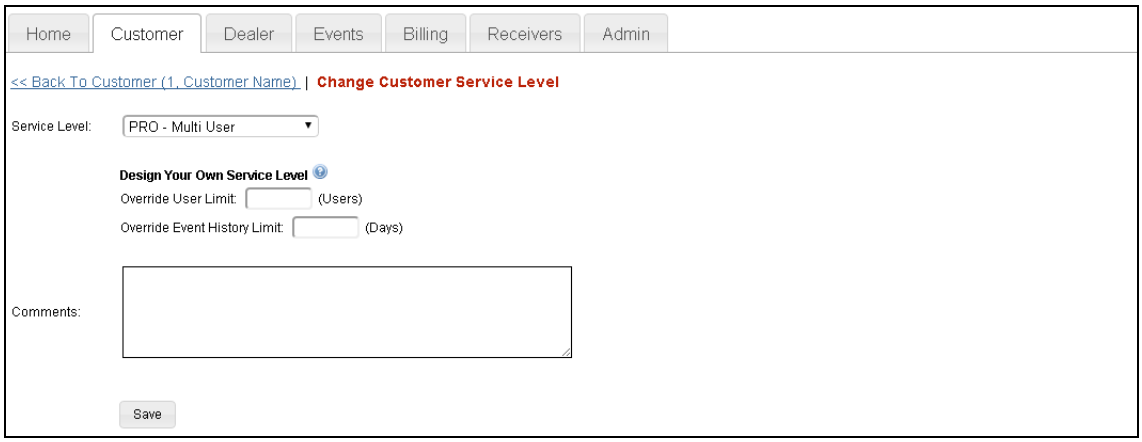
New Customer Setup

1) Login to the Connect ONE Dealer Site, https://www.connectmysites.net.
2) Click on the “Customer” Link.
3) In you area adding a site to an existing customer, click on the existing customer from the list, then click on Sites, lastly “Add a new Site” and skip to step 10. Otherwise for a new customer, click the “Add New Customer” link.
4) Fill-in the required information about this customer.


Customer Dealer Events Billing Receivers
<< Back To Customers | New Customer Information
Dealer: Connected Technologies
Number: 12 - 1234 *
Name: Customer Name *
Address: 123 Anystreet *
City: Anytown
State/Province: IL
Zip/Postal Code: 60000
Country: USA
Admin Email: admin@domain.com
Time Zone: US/Central
Time Format: 12 Hour
The administrator user will be created with the following credentials:
User: admin Password: n3wpa55w0rd
Leave Inactive and Continue
Activate and Continue

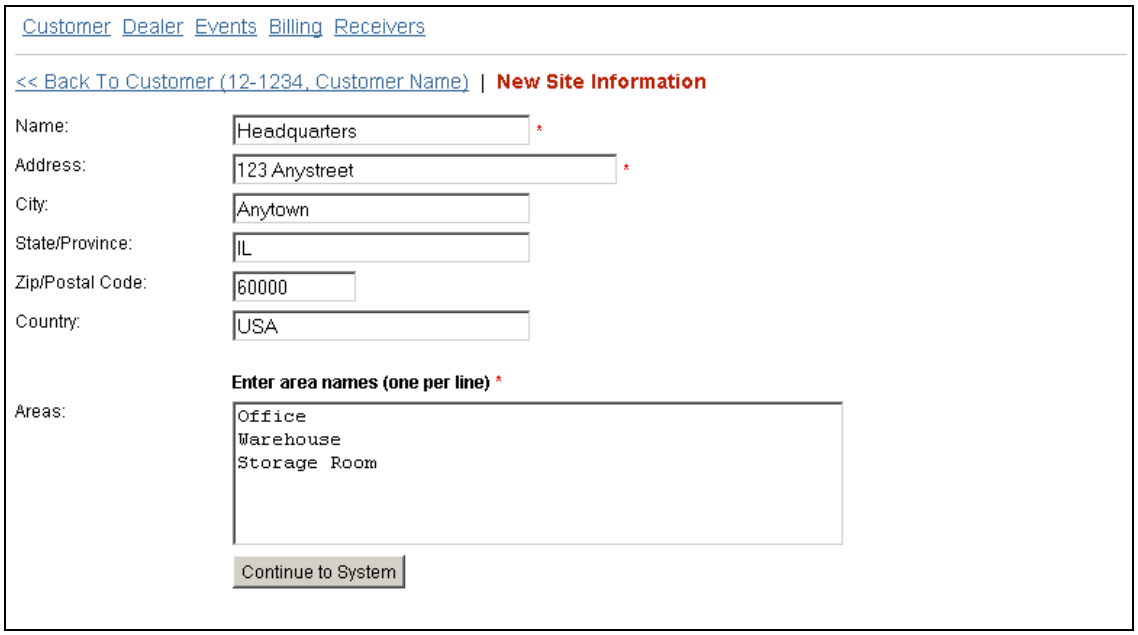
Create Customer Setup Form

5) Your customer will login with the customer number you specify, ex) 12-1234.
6) The time format selection allows your customer to see all times on the website in 12 hour format, 1:34:00 PM, or 24 hour format, 13:34:00.
7) To continue, you may choose to activate the account now, which will start the billing, or to leave inactive if you are setting up this account ahead of the installation, skip to step 10 if leaving inactive.



Activate Customer Form

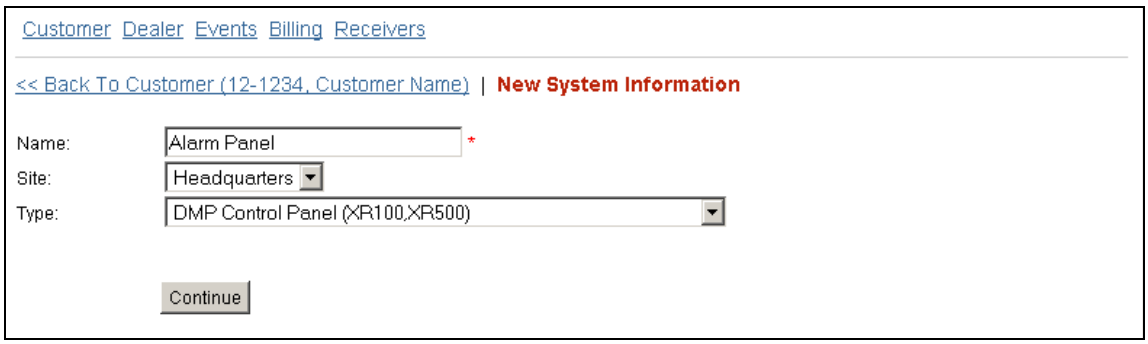
8) Choose the service level from the drop-down window; You may also choose to add any comments.
9) Click “Save”.
NOTE: Design Your Own Service Level allows you to set your own customer limits of max users and event history time length.



Create Site Setup Form

10) Fill-in the required information about this site.
11) Enter the area names to be used for this site, one per line.
12) Click “Continue to System”.

Create a DMP System


Customer Dealer Events Billing Receivers
<< Back To Customer (12-1234, Customer Name) | New System Information
Name: Alarm Panel *
Site: Headquarters
Type: DMP Control Panel (XR100,XR500)
Continue

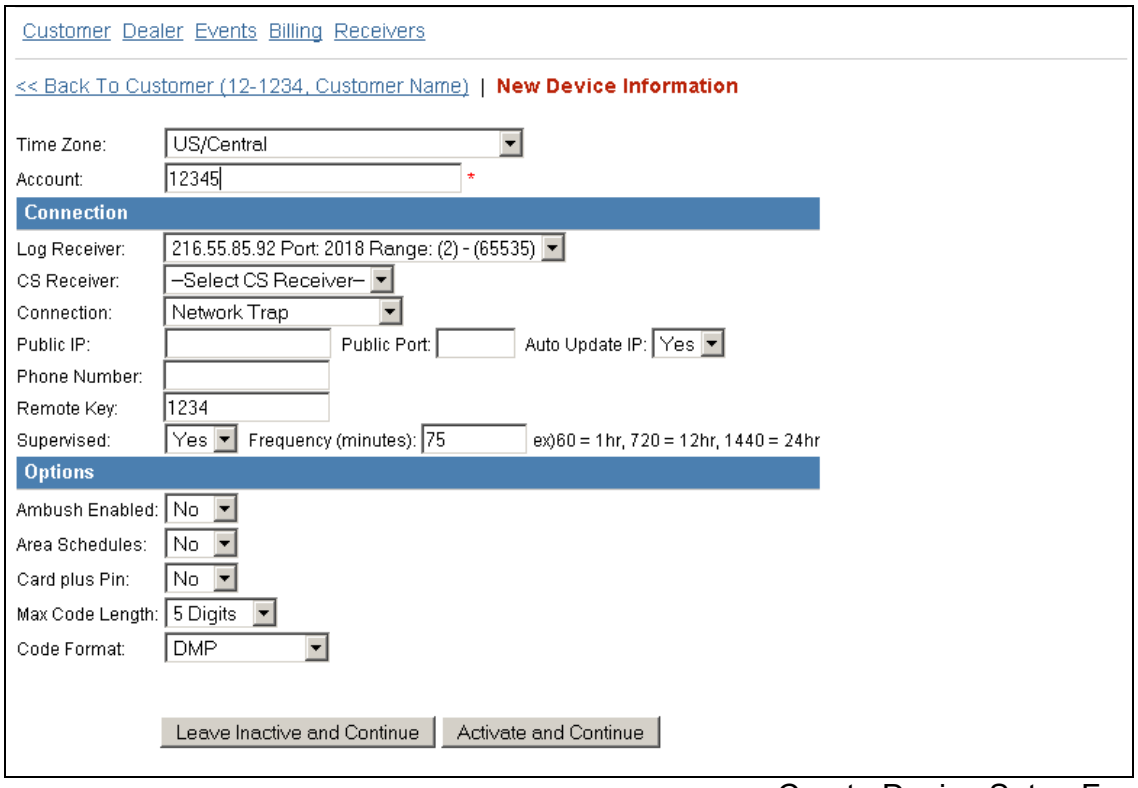
Create System Setup Form

1) Fill-in the required information about this system.
2) Choose the System Type from the drop-down.
3) Click “Continue”.

Customer Dealer Events Billing Receivers
<< Back To Customer (12-1234, Customer Name) | New Device Information
Dealer: Connected Technologies
Type (Version): XR500 (205+)
Continue To Device

Create Device Type Setup Form

4) Choose the Device Type and Version from the drop-down. If you are unsure of the version, the device will correct it upon it communicating any programming commands.
5) Click “Continue to Device”

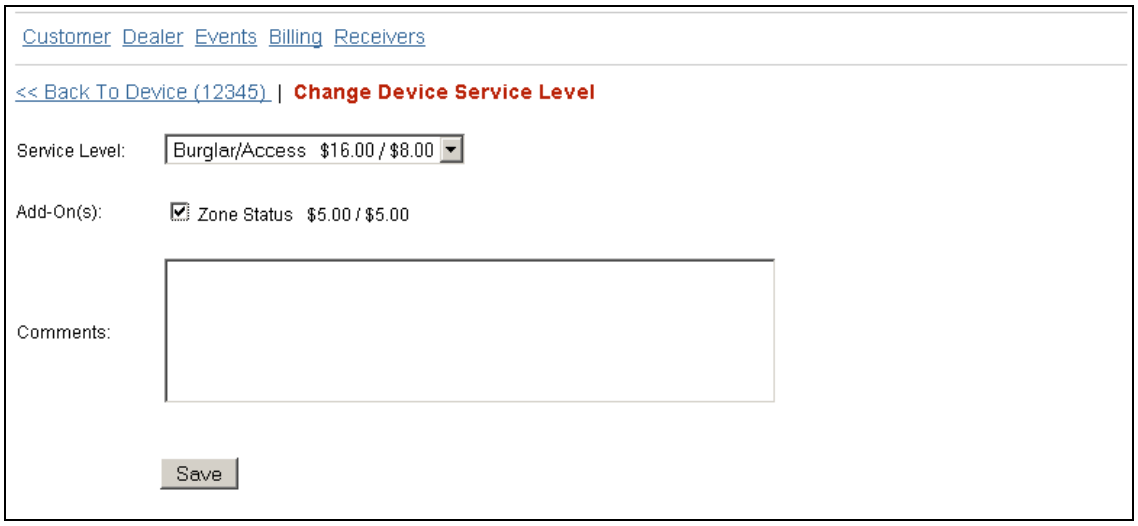

Customer Dealer Events Billing Receivers
<< Back To Customer (12-1234, Customer Name) | New Device Information
Time Zone: US/Central
Account: 12345 *
Connection
Log Receiver: 216.55.85.92 Port: 2018 Range: (2) - (65535)
CS Receiver: –Select CS Receiver–
Connection: Network Trap
Public IP: Public Port: Auto Update IP: Yes
Phone Number:
Remote Key: 1234
Supervised: Yes Frequency (minutes): 75 ex)60 = 1hr, 720 = 12hr, 1440 = 24hr
Options
Ambush Enabled: No
Area Schedules: No
Card plus Pin: No
Max Code Length: 5 Digits
Code Format: DMP
Leave Inactive and Continue
Activate and Continue

Create Device Setup Form

6) Fill-in the required information about this device.
   a. Enter the Account Number
   b. Set Log Receiver - This is the receiver programmed in the panel under PC Log Reports and Communication.
   c. Enter the Remote Key
   d. Choose the Connection Type
      i. DMP Cellular Connect – Direct Connection via DMP Cellular Radio (Uses the Phone location entered below)
      ii. Network Direct Connect – Direct Connection via Network
      iii. Network Trap – Trap the panel via Connect ONE Servers
      iv. Network Trap via CS – Trap the panel via the Central Station Receiver (Uses the CS IP and Port entered below)
   e. Public IP Address, Port, and Auto Update: If the Auto Update IP setting is Yes the public IP address is automatically determined upon the first communication with the panel and updated on each new connection.
   f. Phone Number: Enter the phone number of the DMP Cellular Radio, enter without dashes, ex) 19995551212.
   g. Central Station IP and Port: Enter if relaying signals or using for trapping.

h. Supervise Test: Enter the number of minutes that a test signal (S07) should be received from the panel. Hint: Add a grace time of at least 15 minutes.
i. Ambush Enabled: Yes (User #1: Cannot be used on the website), No (User #1: Can be used as a general code on the website)
j. Area Schedules: Yes (Show shift schedules by area name and show shifts for each area), No (Refer to shift schedules by "shift" and limit to 4)
k. Card plus Pin: Yes (Show field to enter Pin), No (Hide Pin Field)
l. Max Code Length: Display warning if customer attempts to enter a code with a higher length.
m. Code Format: Display warning if customer attempts to enter a code with a higher number than is possible based on this bit length. This is the same number programmed into the keypads. Example: DMP cards and keyfobs (17 Bits), Standard 26-Bit cards and keyfobs (16 Bits).

7) To continue, you may choose to activate the account now, which will start the billing, or to leave inactive if you are setting up this account ahead of the installation, skip to step 12 if leaving inactive.



Activate Device Form

8) Choose the service level from the drop-down.
9) Select any Add-On services.
10) Enter any comments.
11) Click "Save".

12) Program the Control Panel (Refer below based on Type and Version)

XR100/500 Communication Setup (V.205 or greater recommended)
XR150/350/550 Communication Setup (All versions)
Communication Paths:

1) Create a new Path number #7 (Network or Cellular) / Primary
2) Test Report: Yes, Frequency & Time: Dealer Determined
3a) (If Network) Use Checkin: Yes, Check-in: 4
3b) (If Cellular) Use Checkin: No
4) Receiver IP / Port: dealer assigned by Connected Technologies
5) Protocol: TCP
6) Reports: SET ALL TO YES

1) Create a new Path number #8 (Network or Cellular) / Backup
2) Test Report: Yes, Frequency & Time: Dealer Determined
3a) (If Network) Use Checkin: Yes, Adaptive
3b) (If Cellular) Use Checkin: No
4) Receiver IP / Port: dealer assigned by Connected Technologies
5) Protocol: TCP

Remote Options:

1) Remote Disarm: Check

System Reports:

1) Enable All (Ambush by dealer discretion)
2) Enable Access Keypad for each Door Controller Address

Area Information:

1) Enable Open/Close Reports

PC Log Reports: (If Cellular Only – Do not Use)

1) Comm Type: Net
2) Reports: Disable all except Real-Time Status
3) Net IP Address / Port: dealer assigned by Connected Technologies

Device Setup:

1) Set Real-time Status on each Access Door

Output Information:

1) Set Real-time Status on each Output for on/off status to log.

Zone Information: **(ONLY ENABLE IF ZONE STATUS SERVICE ADDON)**

1) Set Real-time Status on each Zone for open/close status log

XT30/50/XTL Communication Setup (V.103 or greater recommended)
For Central Station Accounts, program receiver 1 for your central station and receiver 2 for Connect ONE servers. No relaying of signals is necessary with this panel firmware. Signals can be routed via two redundant paths.

Communication:

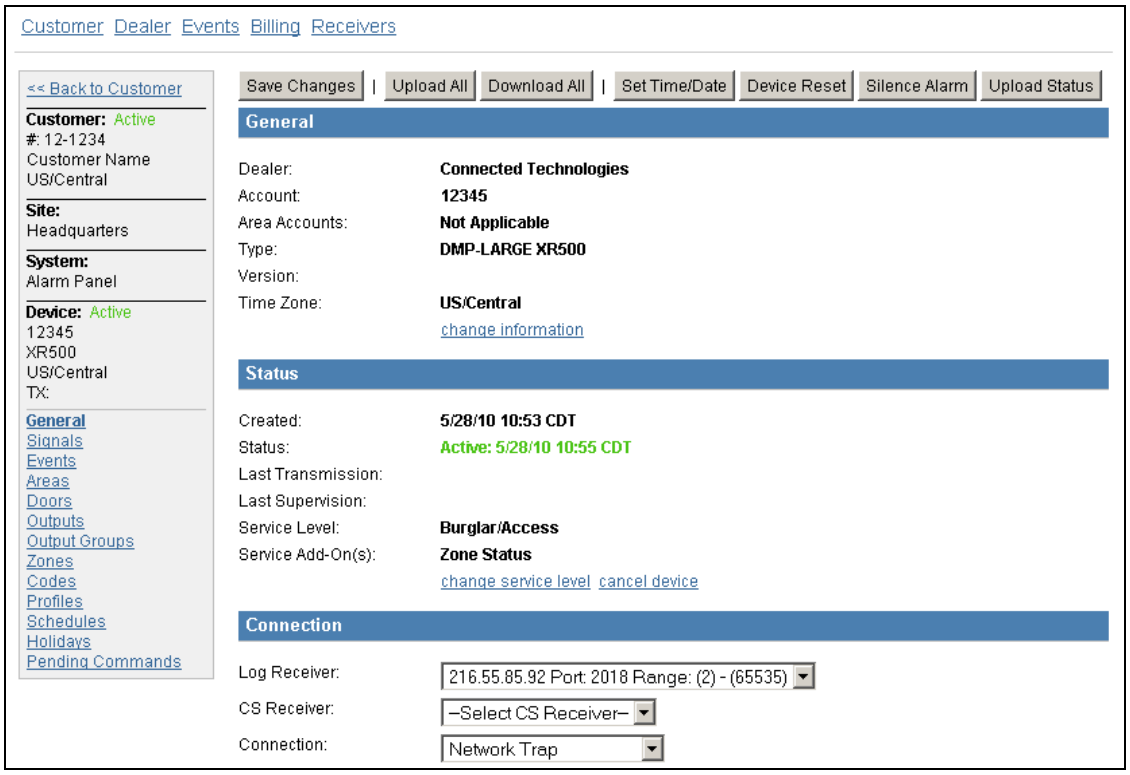
1) Comm Type: Net
2) Test Timer: Test Time & Net Test Days: Dealer Determined
3) Receiver:
    Receiver 1: Check Any Necessary for Central Station
        a. 1st IP Addr: central station or blank
        b. 1st IP Port: central station or blank
    Receiver 2: Check All
        a. 1st IP Addr: dealer assigned by Connected Technologies
        b. 1st IP Port: dealer assigned by Connected Technologies
        c. 2nd IP Addr: dealer assigned by Connected Technologies
        d. 2nd IP Addr: dealer assigned by Connected Technologies
4) Advanced Communications:
    Check-in: 4, 15, or above

Remote Options:

1) Remote Disarm: Yes

System Reports:

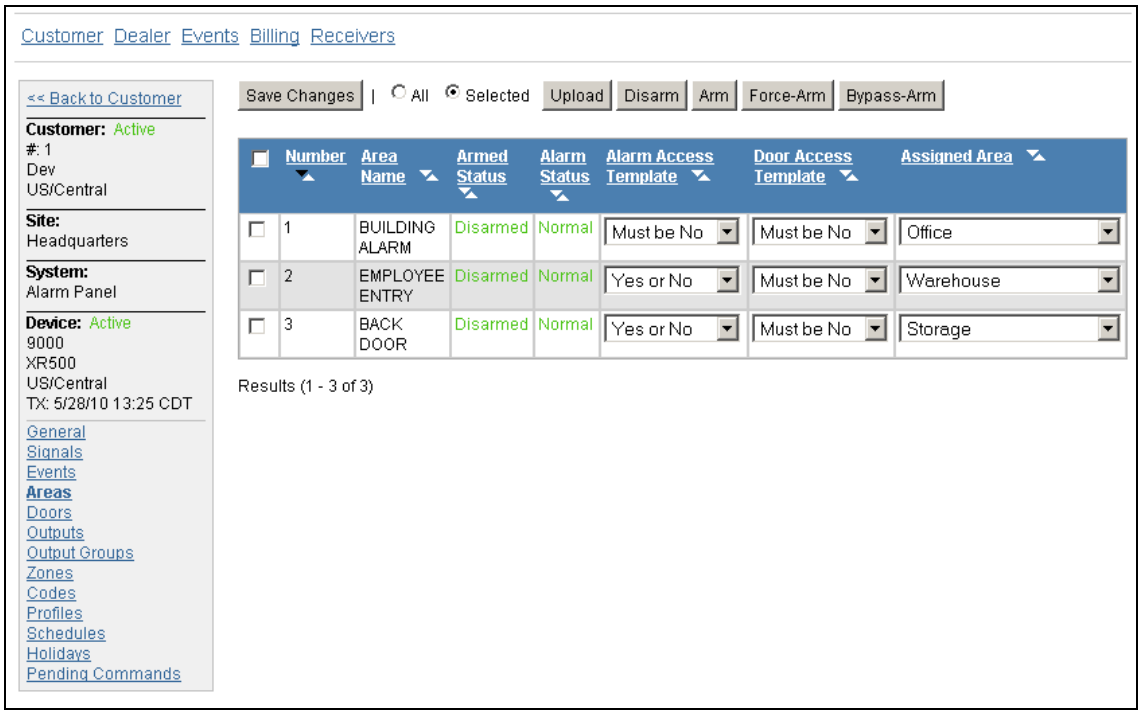
1) Zone Restorals: Yes
2) Open/Close Enable: Yes
3) Check All Others



Device View

13) Click “Receive All”, this will enter the commands to receive all of the necessary information from the control panel. Once the commands have processed, continue through this guide.

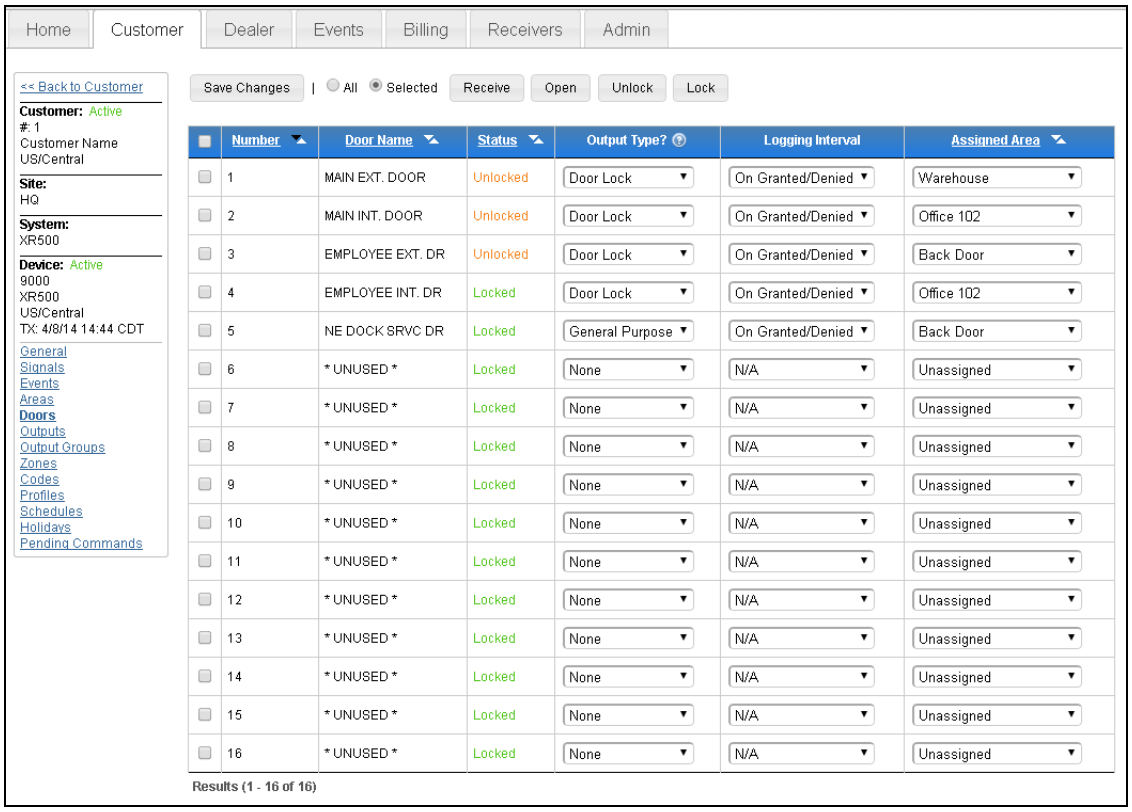
14)Click on “Areas”, the following screen should appear.



Device Areas

15) Assign each device area to a site area using the “Assigned Area” drop-down box.
16) Choose the “Alarm Access” and “Door Access” template option for each area. This can be used for alarm only or common areas. The options are:
    n. Yes or No – The customer may assign yes or no for a profile’s privilege to this area.
    o. Must be No – The customer may not choose yes for a profile’s privilege to this area.
    p. Must be Yes – The customer may not choose no for a profile’s privilege to this area.
17) Click “Save Changes”

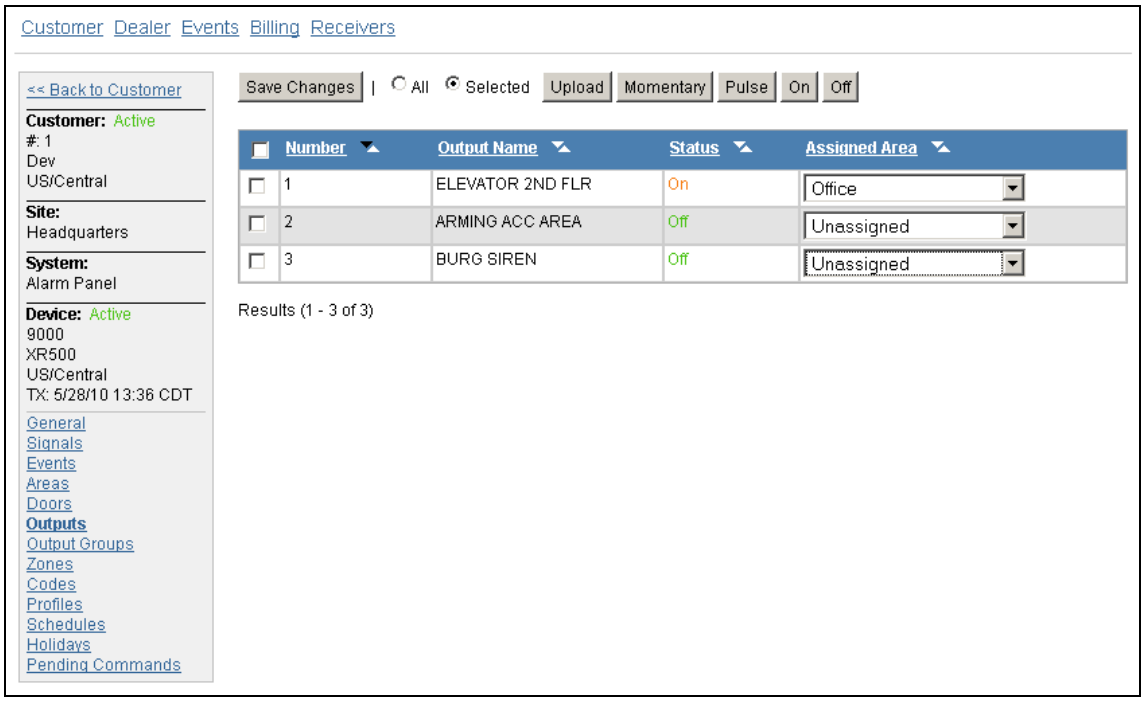
18) Click on “Doors”, the following screen should appear. – IF APPLICABLE



Device Doors

19) Set the Output Type for each door. Door Lock sets the commands to Open, Unlock, Lock, & status to Locked/Unlocked. General Purpose sets the commands to Momentary, On, Off & status to On/Off. None hides the device from any control screens.
20) Set the Logging Interval on each door you want access granted and access denied events logged. Each door selected will reflect in the service level subscribed for this account.
21) Assign each device door to a site area using the “Assigned Area” drop-down box. Only assign doors / keypads that actually are a door controller. Only the doors you assign to an area will show up for the customer as a door. For instance, do not assign keypads without a door controller and zone expanders.
22) Click “Save Changes”

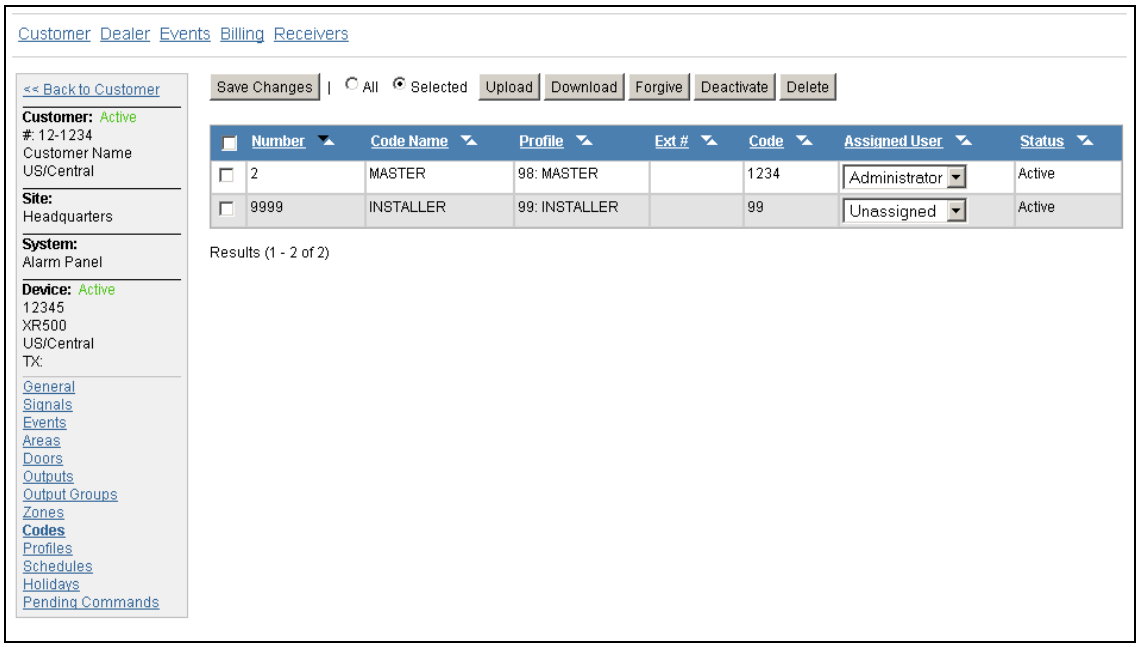
23)Click on “Outputs”, the following screen should appear. – IF APPLICABLE



Device Outputs

24) Assign each device output to a site area using the “Assigned Area” drop-down box. Only assign outputs that you want the customer to have control over. For instance, do not assign outputs that trip a radio.
25) Click “Save Changes”

26)Click on “Codes”, the following screen should appear.



Device Codes

27) Assign the master level code to the Administrator user. This gives the system level permissions to the Administrator. These permissions are on the profile or authority level of the code you are assigning. For instance, arming/disarming, modify system codes, profiles, schedules, etc.
28) Click “Save Changes”

XR100/150/350/500/550 Notes:

- Recommended Setup
  - Create a Master Profile #98, with all permissions enabled except only assign areas programmed for alarm and access area options. In this example profile 98 should only have areas 1-3 for alarm and access.
  - The Installer Profile #99 should remain default with all areas, 1-32 enabled for alarm and access areas.
  - This setup ensures that your installer code will not be seen by your customer since their profile 98 has less areas of authority.

Setup Complete!

Advanced Access Control with DMP

This explains how to configure each access door as its own area while still allowing the customer easy use at the site and easy management of profiles.

Equipment: XR100/500, 305 Relay, 431 Harness, 7063 Keypad, 734 Door Controllers

Area Information:
Set Any Bypass to Yes
1: Alarm, Armed Output: 1
2: Front Door
3: Rear Door

Device Setup:
1: Keypad, Display Area: 1
2: Front Door, Display Area: 1, Access Areas: 1-2, Real-Time Status: Yes, Override: Yes
3: Rear Door, Display Area: 1, Access Areas: 1&3, Real-Time Status: Yes, Override: Yes

Output Information:
1: Arm Access Areas, Real-Time Status: Yes

Zone Information:
1: Arm Access Areas, Set to Arming Type: Maintain, Arm Areas: 2-3

Profiles:
97: All Access when Disarmed, Access Areas: 2-3, Alarm Areas: None
98: Master, Access Areas 2-3, Alarm Areas: 1-3

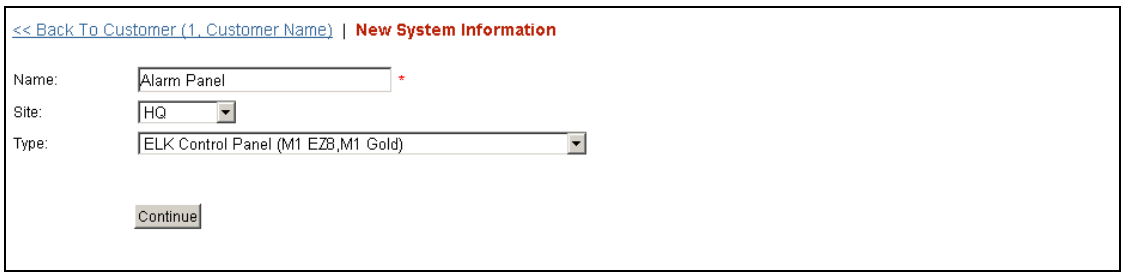
A key point to remember is that with a door controller the key field in Device Setup is Access Areas. A user only needs to match one of the areas to be granted access. So in this setup the users will be matched to the access areas 2 and 3 and not 1 however once granted access the panel will attempt to disarm all access areas listed, so 1-3 will be disarmed if the user's profile has 1-3 set in the alarm areas listing of the profile. Since override is set and we are arming all areas with the keyswitch zone the door will also lock upon arming in this configuration.

Also, another key point is that area 1 should never be listed in the access areas list of any user profile. To prevent this from happening by your customer set the Door Access Template to "Must be No", for that Area on the Dealer Site.

Any Bypass is turned on; this will ensure that in all circumstances the arm access areas output will turn on. This output is what will give you the override feature since it will arm the access areas with the alarm area. To do the arming, wire the output to short zone 1 or any zone you have configured as an arming zone. This makes it simple for your end user also because now at the keypad it will only show area 1 not the access areas. The access areas should also be set to “Do Not Show” on the Dealer Site. This will hide them on the Monitor->Alarm/Access Areas page, just like on the keypad, however it will still show them when editing a System Profile.

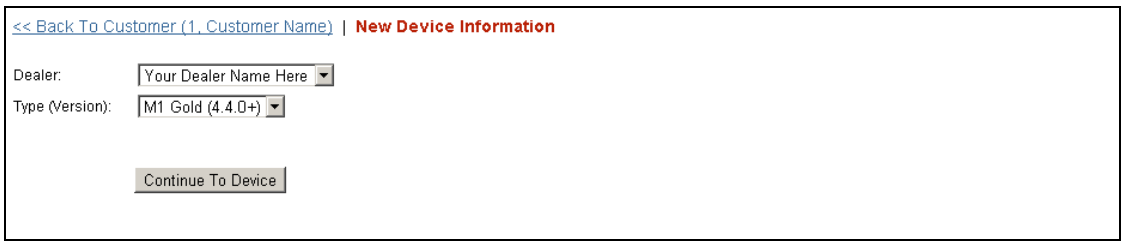
Create an ELK System

- RP Version 2.0.16 or higher required
- M1 Version 5.2.8 or higher required
- XEP Version 2.09 or higher required, firmware can be downloaded at http://www.elkproducts.com/M1Cloud



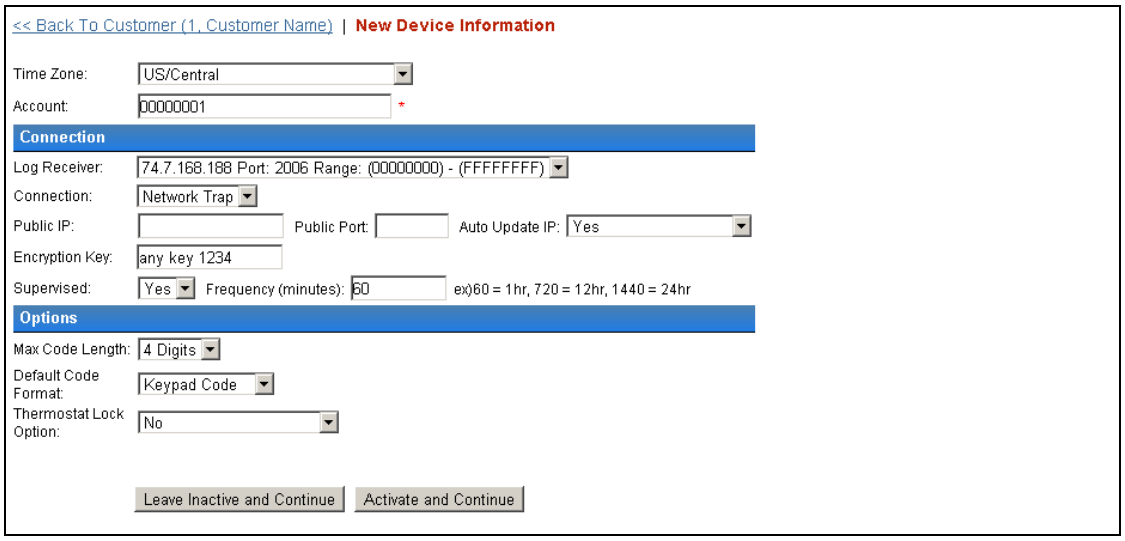
Create System Setup Form

1) Fill-in the required information about this system.
2) Choose the System Type from the drop-down.
3) Click “Continue”.


<< Back To Customer (1, Customer Name) | New Device Information
Dealer:
Your Dealer Name Here
Type (Version):
M1 Gold (4.4.0+)
Continue To Device

Create Device Type Setup Form

4) Choose the Device Type and Version from the drop-down. If you are unsure of the version, the device will correct it upon it communicating any programming commands.
5) Click “Continue to Device”


<< Back To Customer (1, Customer Name) | New Device Information
Time Zone: US/Central
Account: 00000001 *
Connection
Log Receiver: 74.7.168.188 Port: 2006 Range: (00000000) - (FFFFFFFF)
Connection: Network Trap
Public IP: Public Port: Auto Update IP: Yes
Encryption Key: any key 1234
Supervised: Yes Frequency (minutes): 60 ex)60 = 1hr, 720 = 12hr, 1440 = 24hr
Options
Max Code Length: 4 Digits
Default Code Format: Keypad Code
Thermostat Lock Option: No
Leave Inactive and Continue
Activate and Continue

Create Device Setup Form

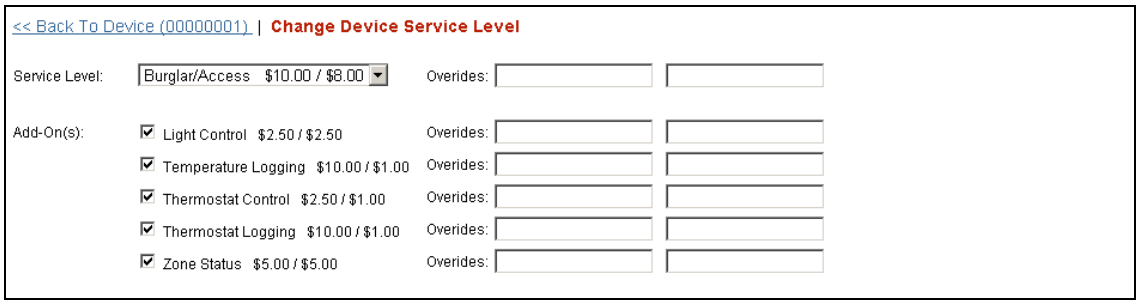
6) Fill-in the required information about this device.
   q. Enter the Account ID, this obtained from ELK RP Software
      i. Open the panel account in RP
      ii. Go to Setup->M1 Cloud
      iii. Click Next, then click Obtain Account ID
   r. Public IP Address, Port, and Auto Update: If the Auto Update IP setting is Yes the public IP address is automatically determined upon the first communication with the panel and updated on each new connection.
   s. Encryption Key: Enter any character string you want to use for this account's encryption key
   t. Supervise Test: Enter the number of minutes that a signal should be received from the panel. Hint: Add a grace time of at least 15 minutes.
   u. Max Code Length: Display warning if customer attempts to enter a code with a higher length.
   v. Default Code Format: Enter the format you wish to be the default when your customer adds a new code.
   w. Thermostat Lock Option: Allows an option to turn on the display lock for thermostats. This does require an M1 Rule to work correctly.
      i. RCS Thermostats – Add these Text Strings:
         1. "<cloud>LT#</cloud>^M^J"
            a. Replace the # place holder with the thermostat number and be sure to insert Carriage Return/Line Feed to generate the ^M^J part of the string.
         2. "<cloud>UT#</cloud>^M^J"
            a. Replace the # place holder with the thermostat number and be sure to insert Carriage Return/Line Feed to generate the ^M^J part of the string.

3. ">A=#,O=0,DL=1^M"
    a. Replace the # place holder with the thermostat number and be sure to insert Carriage Return to generate the ^M part of the string.
4. ">A=#,O=0,DL=0^M"
    a. Replace the # place holder with the thermostat number and be sure to insert Carriage Return to generate the ^M part of the string.

ii. RCS Thermostats – Create these Rules:

1. WHENEVER THE FOLLOWING TEXT IS RECEIVED: "<cloud>LT#</cloud>^M^J" THROUGH PORT 0 THEN SEND THE FOLLOWING TEXT: ">A=#,O=0,DL=1^M" THROUGH PORT 1
    a. Enter the correct port number for the M1XSP, this example uses port 1.
2. WHENEVER THE FOLLOWING TEXT IS RECEIVED: "<cloud>UT#</cloud>^M^J" THROUGH PORT 0 THEN SEND THE FOLLOWING TEXT: ">A=#,O=0,DL=0^M" THROUGH PORT 1
    a. Enter the correct port number for the M1XSP, this example uses port 1.

7) To continue, you may choose to activate the account now, which will start the billing, or to leave inactive if you are setting up this account ahead of the installation, wait to proceed to step 12 until you activate the account.


<< Back To Device (00000001) | Change Device Service Level
Service Level: Burglar/Access $10.00 / $8.00 Overides:
Add-On(s): Light Control $2.50 / $2.50 Overides:
Temperature Logging $10.00 / $1.00 Overides:
Thermostat Control $2.50 / $1.00 Overides:
Thermostat Logging $10.00 / $1.00 Overides:
Zone Status $5.00 / $5.00 Overides:

Activate Device Form

8) Choose the service level from the drop-down.
9) Select any Add-On services.
10) Enter any comments.
11) Click "Save".

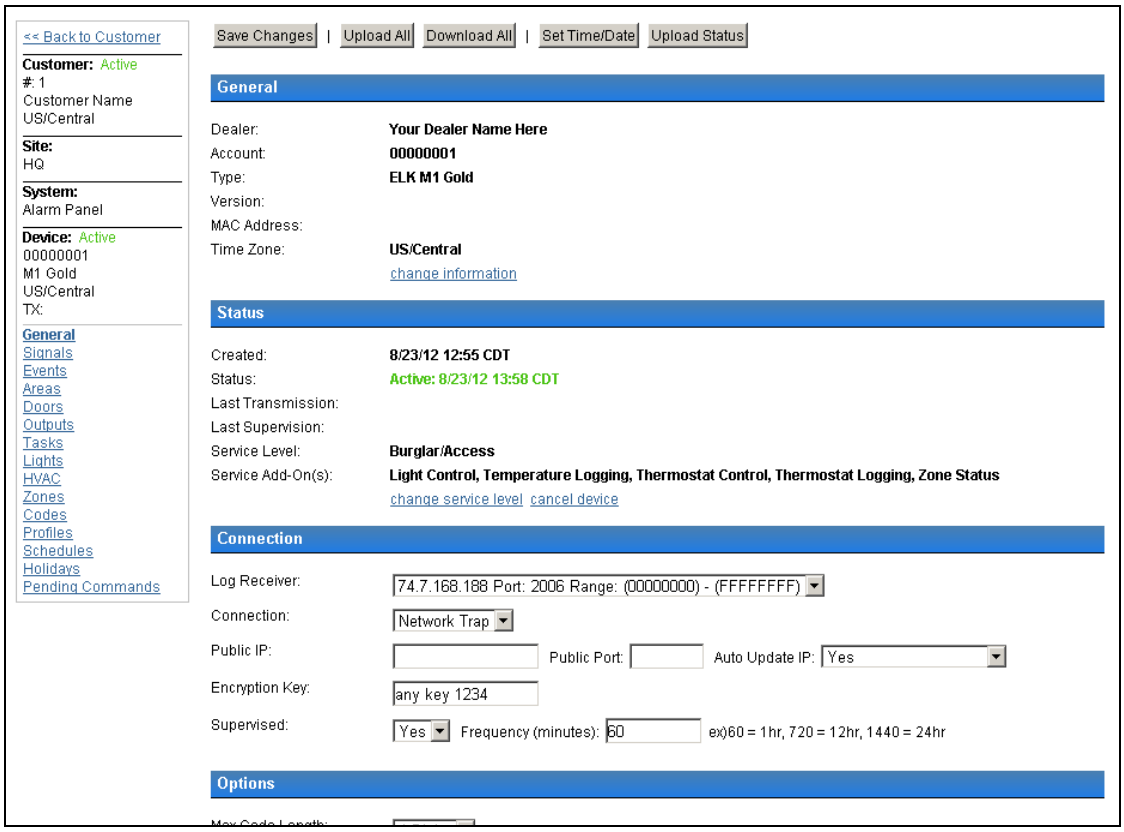
Program the Control Panel

12) Connect to the Control Panel via ELK RP with the proper access code set. The access code gets stored upon this connection for later use with Connect ONE.

Globals->Special Tab:
1) Enable All Serial Port 0 Transmit Options
M1XEP Setup->TCP/IP Settings Tab:
1) Ensure you have a valid DNS server assigned

General Notes:
Every 60 seconds a message is sent from the control panel to Connect ONE. During this periodic message is when any pending commands will be processed. This provides easier networking configuration and better security since the customer's firewall does not need to be opened for an incoming connection.

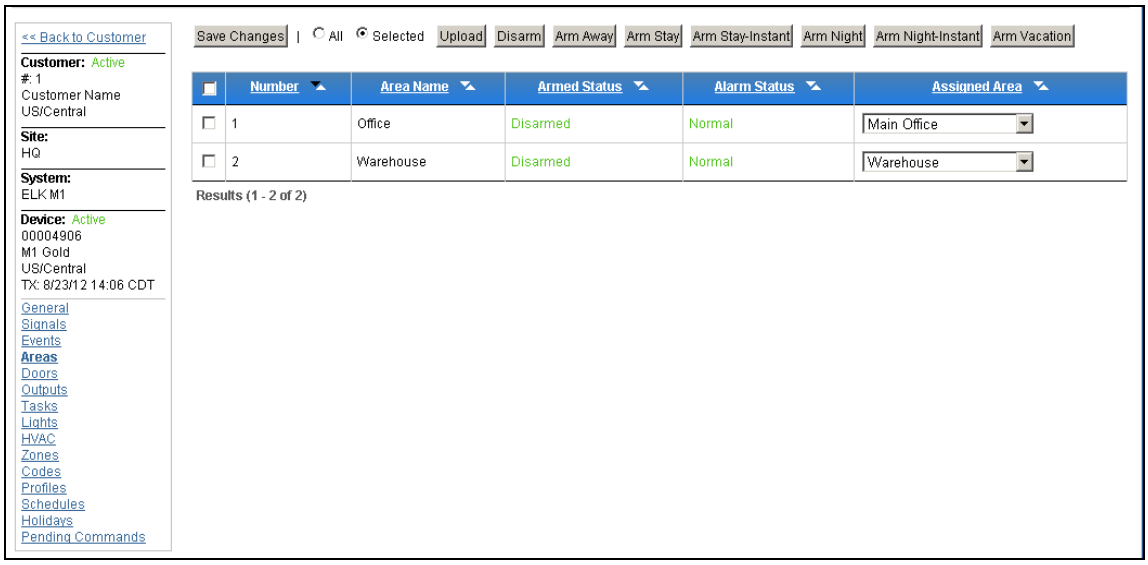
Upon first communication and once per day from then on the control panel time will be synched via Connect ONE.



Device View

13) Click “Receive All”, this will enter the commands to receive all of the necessary information from the control panel. Once the commands have processed, continue through this guide.

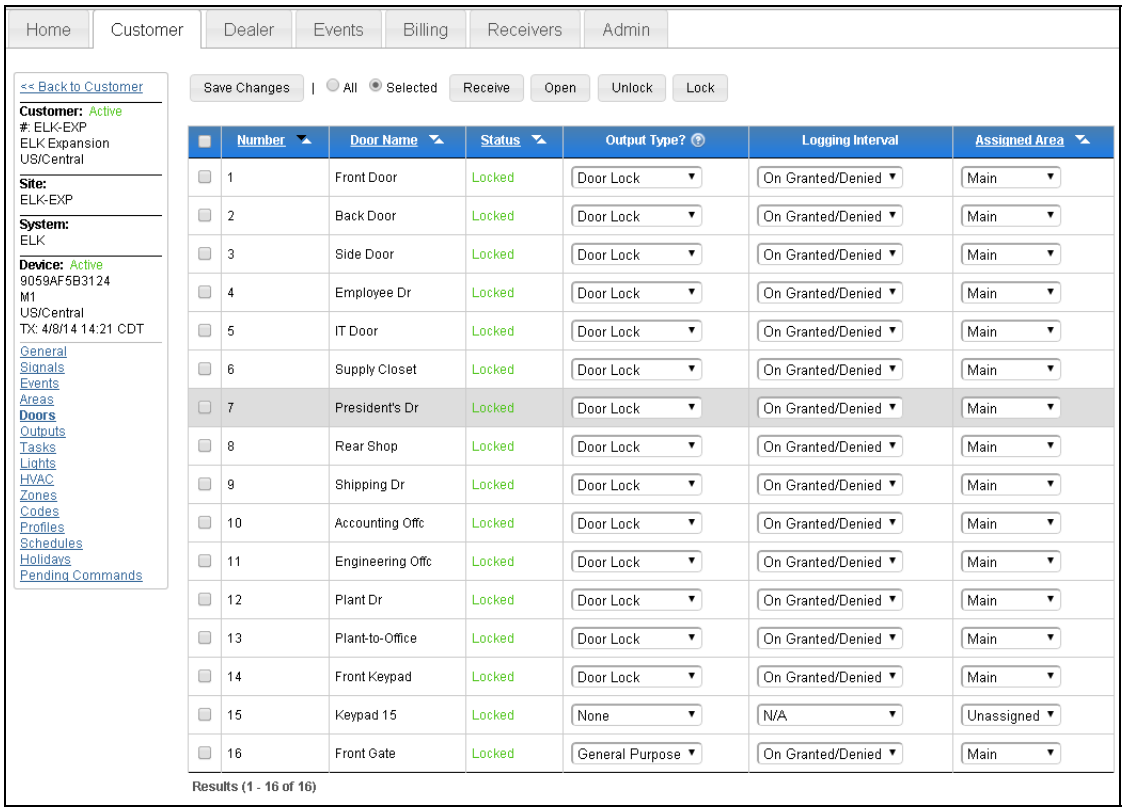
14)Click on “Areas”, the following screen should appear.



Device Areas

15) Assign each device area to a site area using the “Assigned Area” drop-down box.
16) Click “Save Changes”

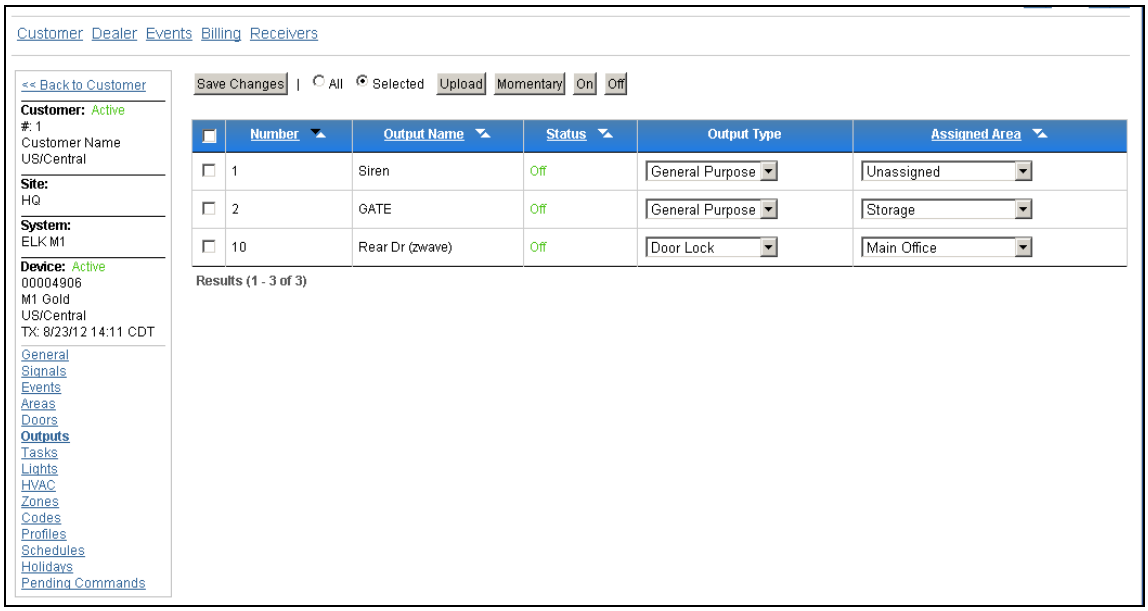
17) Click on “Doors”, the following screen should appear. – IF APPLICABLE



Device Doors

18) Set the Output Type for each door. Door Lock sets the commands to Open, Unlock, Lock, & status to Locked/Unlocked. General Purpose sets the commands to Momentary, On, Off & status to On/Off. None hides the device from any control screens.
19) Set the Logging Interval on each door you want access granted and access denied events logged. Each door selected will reflect in the service level subscribed for this account.
20) Assign each keypad & device door to a site area using the “Assigned Area” drop-down box.
21) Click “Save Changes”

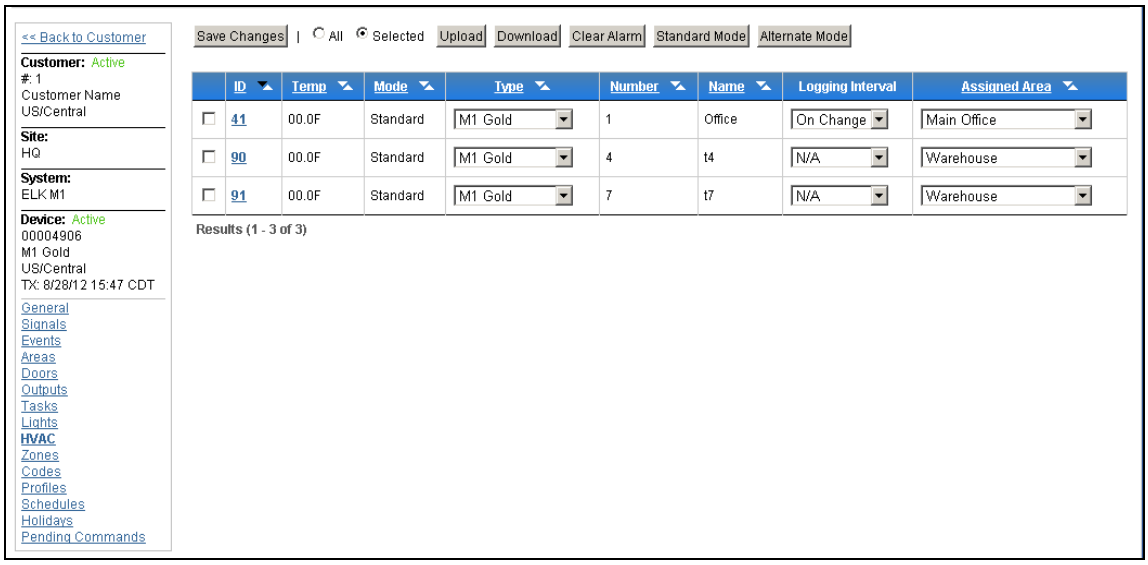
22) Click on “Outputs”, the following screen should appear. – IF APPLICABLE



Device Outputs

23) Assign each device output to a site area using the “Assigned Area” drop-down box. Only assign outputs that you want the customer to have control over. For instance, do not assign outputs that trip a radio.
24) If the output is a connected to a door lock, set it as that type. This makes the status of the output appear as locked/unlocked instead of on/off.
25) If the output is a z-wave door lock add the following M1 rules:
    x. WHENEVER Out 10 STATE IS TURNED ON THEN SEND THE FOLLOWING TEXT: “<ULOCK1^M” THROUGH PORT 2
        i. Replace the output number with the actual output used, replace the lock number with the actual zwave lock number, and use the proper port number assigned to the M1XSLZW
    y. WHENEVER Out 10 STATE IS TURNED OFF THEN SEND THE FOLLOWING TEXT: “<LOCK1^M” THROUGH PORT 2
        i. Replace the output number with the actual output used, replace the lock number with the actual zwave lock number, and use the proper port number assigned to the M1XSLZW
26) Click “Save Changes”

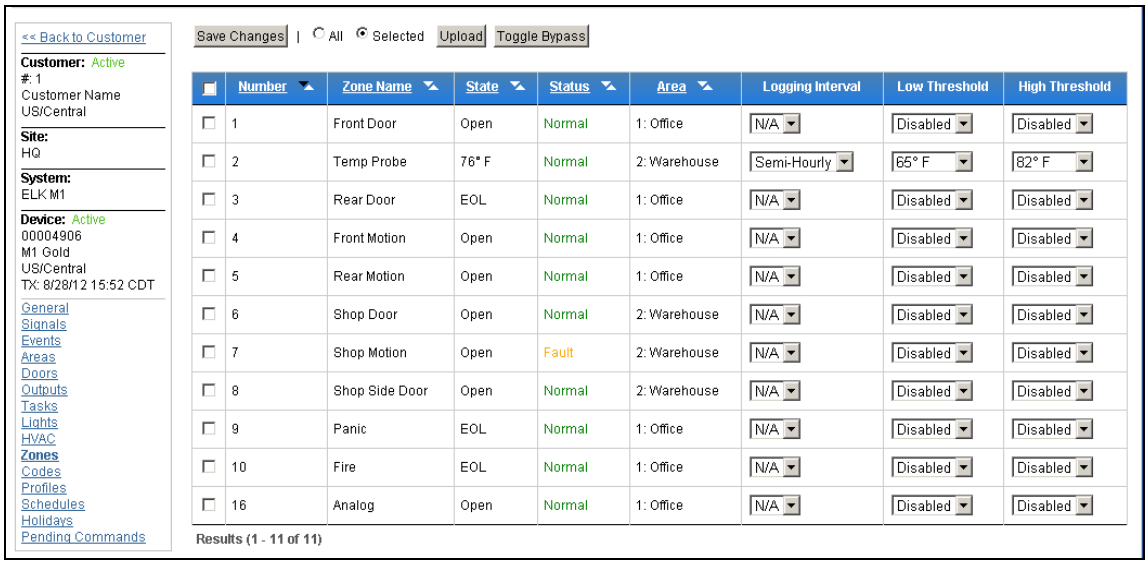
27)Click on “HVAC”, the following screen should appear.



Device HVAC

28) Set the logging interval if applicable. The thermostat logging service level needs to be selected for this option. If selected upon each thermostat change the information will be logged for retrieval in a graphical statistical report.
29) Assign the thermostats to a site area using the “Assigned Area” drop-down box.
30) Click “Save Changes”

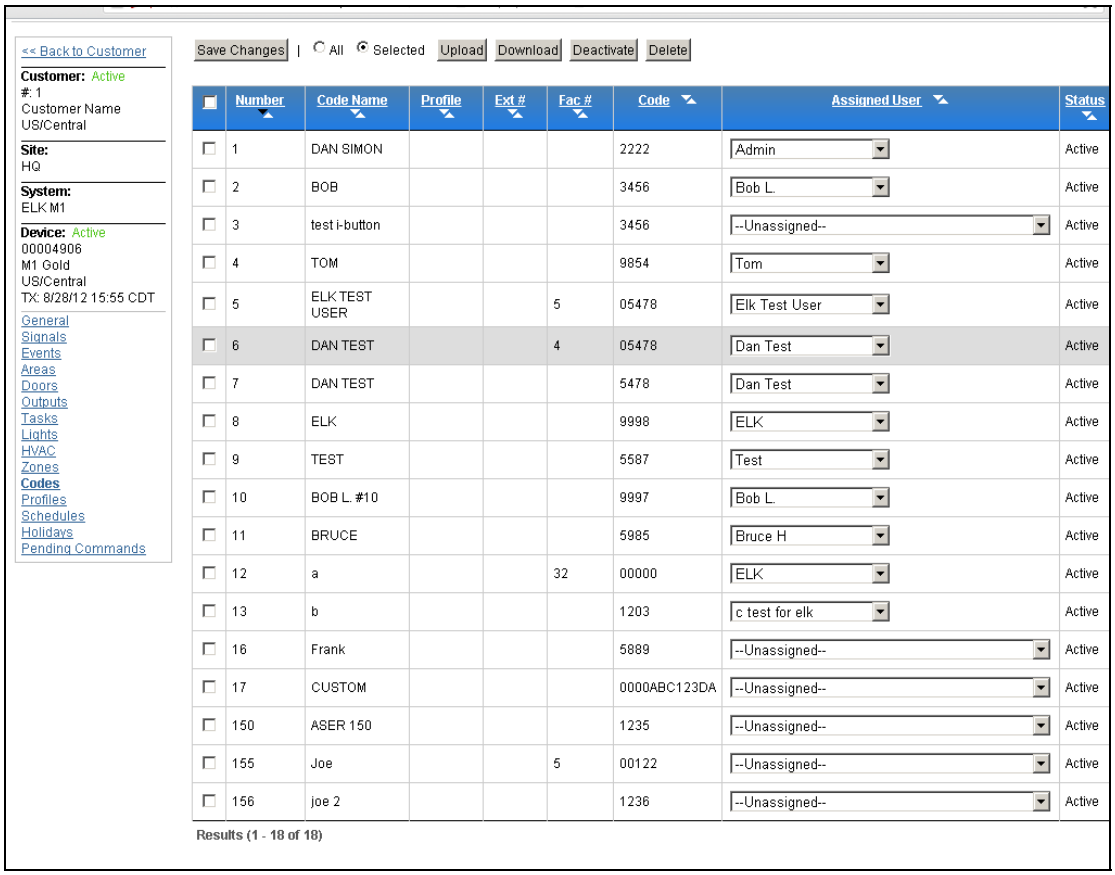
31)Click on “Zones”, the following screen should appear.


<< Back to Customer
Customer: Active
#: 1
Customer Name
US/Central
Site:
HQ
System:
ELK M1
Device: Active
00004906
M1 Gold
US/Central
TX: 8/28/12 15:52 CDT
General
Signals
Events
Areas
Doors
Outputs
Tasks
Lights
HVAC
Zones
Codes
Profiles
Schedules
Holidays
Pending Commands
Save Changes | All Selected Upload Toggle Bypass
Number Zone Name State Status Area Logging Interval Low Threshold High Threshold
1 Front Door Open Normal 1: Office N/A Disabled Disabled
2 Temp Probe 76° F Normal 2: Warehouse Semi-Hourly 65° F 82° F
3 Rear Door EOL Normal 1: Office N/A Disabled Disabled
4 Front Motion Open Normal 1: Office N/A Disabled Disabled
5 Rear Motion Open Normal 1: Office N/A Disabled Disabled
6 Shop Door Open Normal 2: Warehouse N/A Disabled Disabled
7 Shop Motion Open Fault 2: Warehouse N/A Disabled Disabled
8 Shop Side Door Open Normal 2: Warehouse N/A Disabled Disabled
9 Panic EOL Normal 1: Office N/A Disabled Disabled
10 Fire EOL Normal 1: Office N/A Disabled Disabled
16 Analog Open Normal 1: Office N/A Disabled Disabled
Results (1 - 11 of 11)

Device Zones

32) Temperature Probes Only: Set the logging interval if applicable. The zone logging service level needs to be selected for this option. If selected upon interval selected the temperature will be logged for retrieval in a graphical statistical report.
33) Temperature Probes Only: Set the low and high threshold levels. If level is reached a low or high temperature alarm event will be generated.
34) Click “Save Changes”

Click on “Codes”, the following screen should appear.

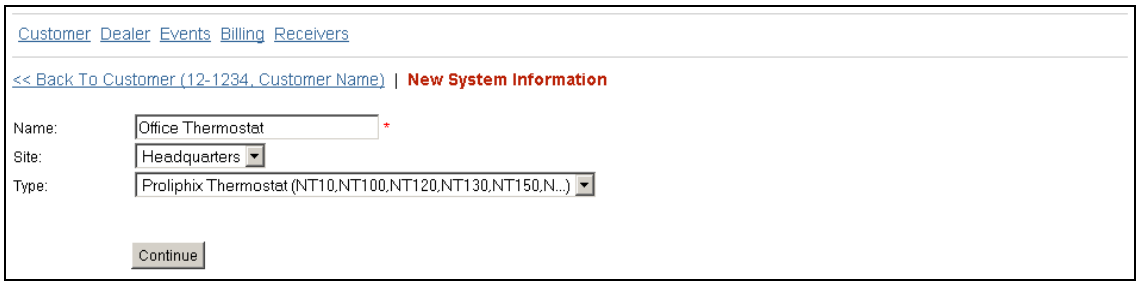


Device Codes

35) Assign the master level code to the Administrator user. This gives the system level permissions to the Administrator. These permissions are on the profile or authority level of the code you are assigning. For instance, arming/disarming, modify system codes, etc.
36) Click “Save Changes

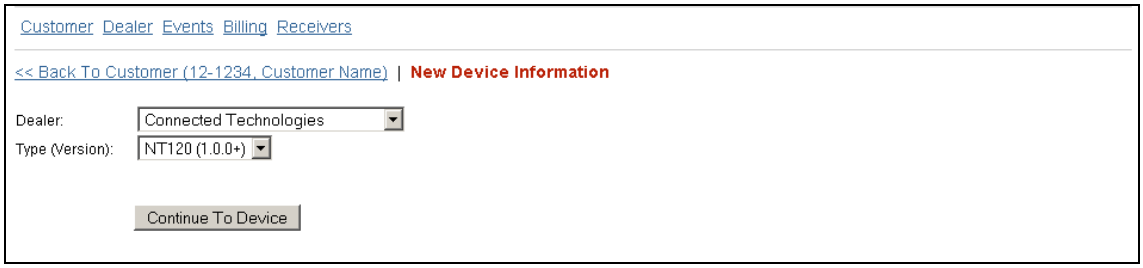
Setup Complete!

Create a Proliphix System


Customer Dealer Events Billing Receivers
<< Back To Customer (12-1234, Customer Name) | New System Information
Name: Office Thermostat *
Site: Headquarters
Type: Proliphix Thermostat (NT10,NT100,NT120,NT130,NT150,N...)
Continue

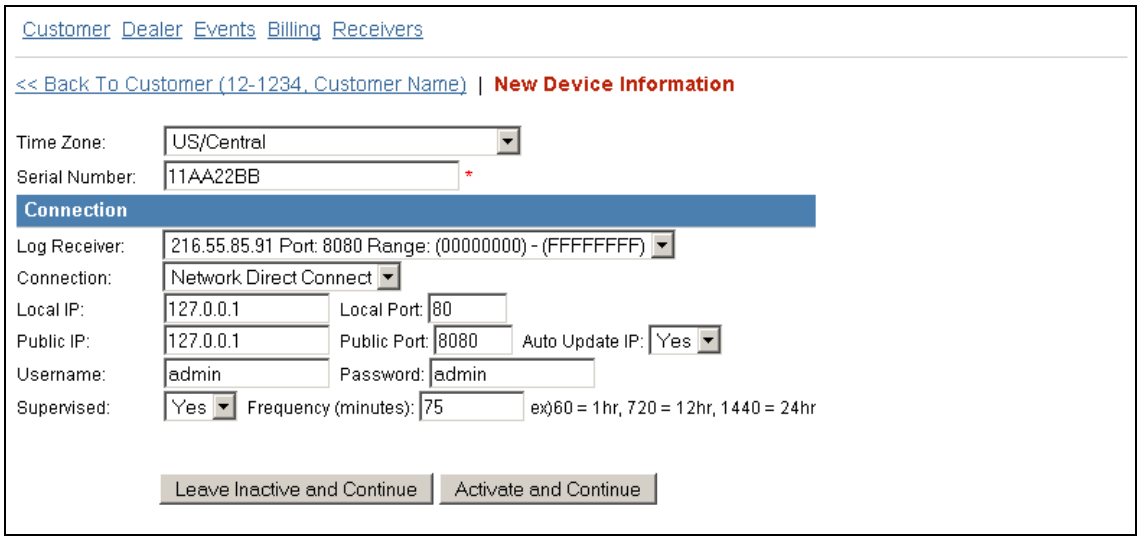
Create System Setup Form

1) Fill-in the required information about this system.
2) Choose the System Type from the drop-down.
3) Click “Continue”.


Customer Dealer Events Billing Receivers
<< Back To Customer (12-1234, Customer Name) | New Device Information
Dealer: Connected Technologies
Type (Version): NT120 (1.0.0+)
Continue To Device

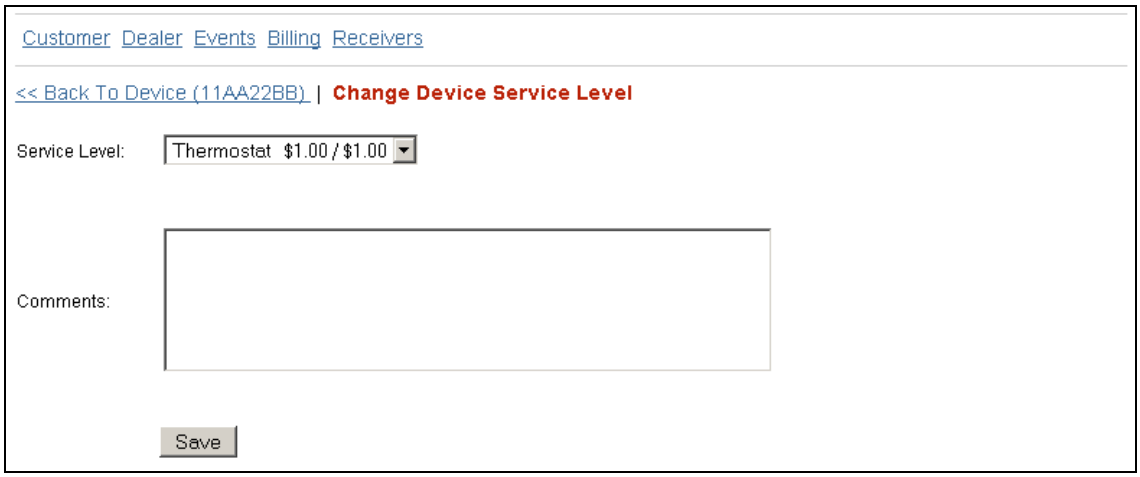
Create Device Type Setup Form

4) Choose the Device Type and Version from the drop-down. If you are unsure of the version, the device will correct it upon it communicating any programming commands.
5) Click “Continue to Device”


Customer Dealer Events Billing Receivers
<< Back To Customer (12-1234, Customer Name) | New Device Information
Time Zone: US/Central
Serial Number: 11AA22BB *
Connection
Log Receiver: 216.55.85.91 Port: 8080 Range: (00000000) - (FFFFFFFF)
Connection: Network Direct Connect
Local IP: 127.0.0.1 Local Port: 80
Public IP: 127.0.0.1 Public Port: 8080 Auto Update IP: Yes
Username: admin Password: admin
Supervised: Yes Frequency (minutes): 75 ex)60 = 1hr, 720 = 12hr, 1440 = 24hr
Leave Inactive and Continue
Activate and Continue

Create Device Setup Form

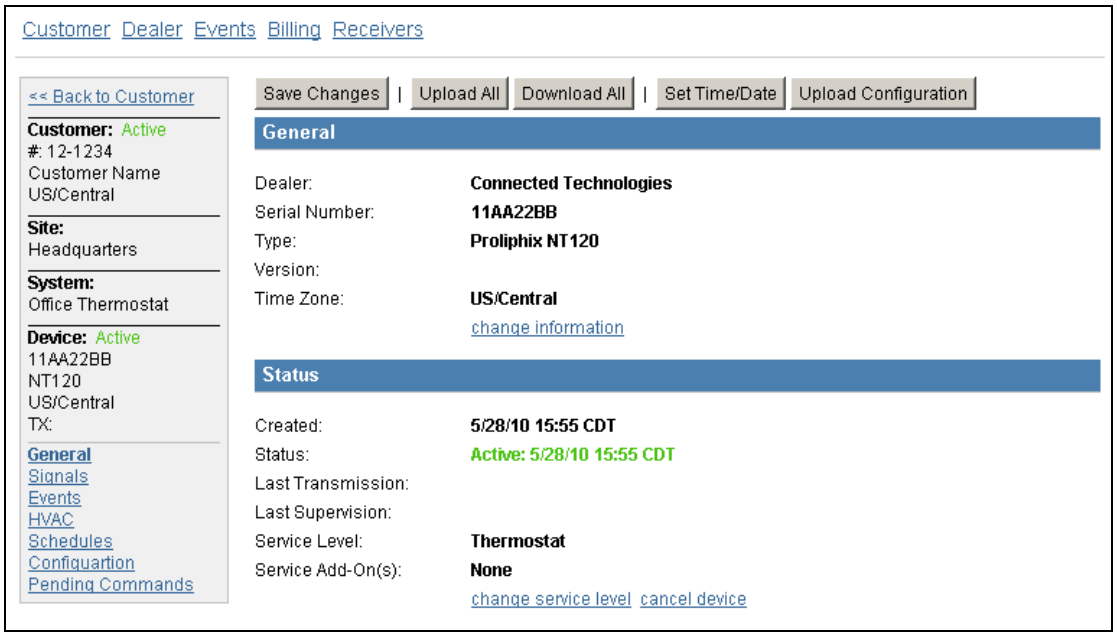
6) Fill-in the required information about this device.
   z. Enter the Serial Number, No dashes.
   aa. Set Log Receiver - This is the receiver programmed in the thermostat under Remote Access.
   bb. Choose the Connection Type
      i. Network Direct Connect – Direct Connection via Network
   cc. Local IP Address & Port – This may be left blank for now and will be updated when using the “Receive All” button on the next screen.
   dd. Public IP Address, Port, and Auto Update: Specify these values so that the initial Receive All commands can process. If the Auto Update IP setting is Yes the Public IP address is updated on each new connection.
   ee. Username & Password: Enter the username and passoword programmed in the thermostat, default: admin for both.
   ff. Supervise Test: Enter the number of minutes that a test signal should be received from the thermostat. Hint: Add a grace time of at least 15 minutes.
7) To continue, you may choose to activate the account now, which will start the billing, or to leave inactive if you are setting up this account ahead of the installation, skip to step 11 if leaving inactive.



Activate Device Form

8) Choose the service level from the drop-down.
9) Enter any comments.
10) Click “Save”.

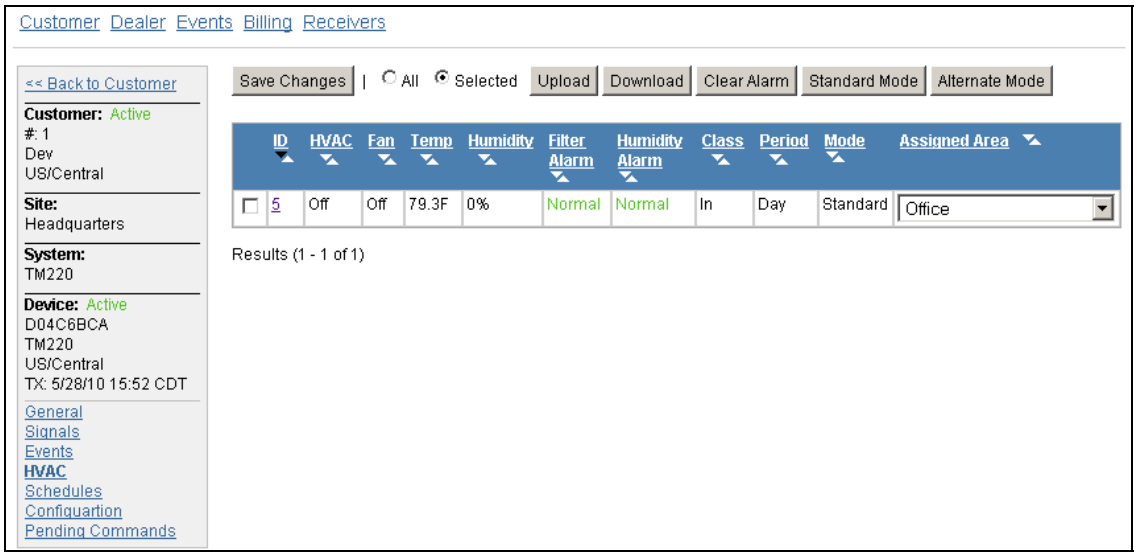
11) Power-up Thermostat
12) Serial # from Box Label: _____
13) View Network Status from Thermostat, IP Address:_____
14) From a web browser go to, http://IP Address
15) Click on “Login”, enter “admin” for username and “admin” for password
    gg. Click on “General Settings”
        i. Enter Device Name (Shows on Display of Unit)
        ii. Turn Off DST Settings (Uncheck)
    hh. Click on “Network Settings”
        i. Enter Firewall Inbound Port, be sure to setup for public access in the router
    ii. Click on “Advanced Settings”
        i. Set HVAC Type
    jj. Click on “Remote Access”
        i. Server Address: dealer assigned by Connected Technologies
        ii. Server Port: dealer assigned by Connected Technologies
    kk. Click Submit, and then click Discover Now



Device View

16) Click “Receive All”, this will enter the commands to receive all of the necessary information from the control panel. Once the commands have processed, continue through this guide.

17) Click on “HVAC”, the following screen should appear.

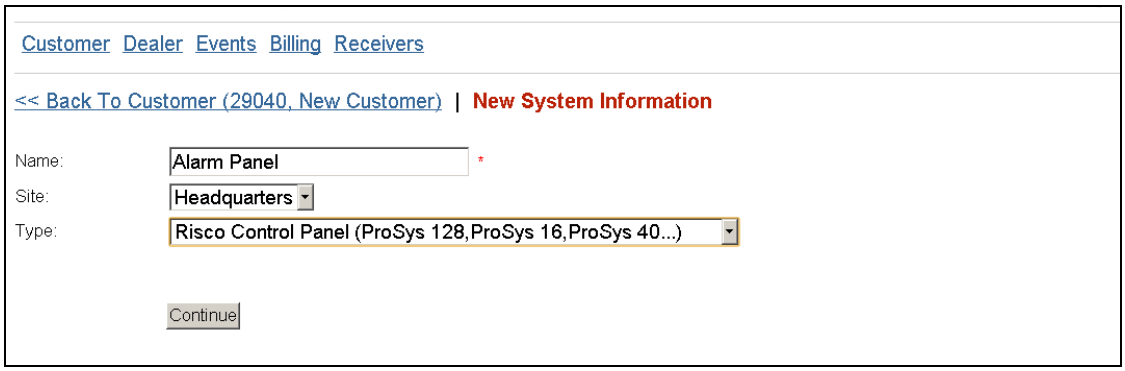


Device HVAC

18) Assign the thermostat to a site area using the “Assigned Area” drop-down box.
19) Click “Save Changes”

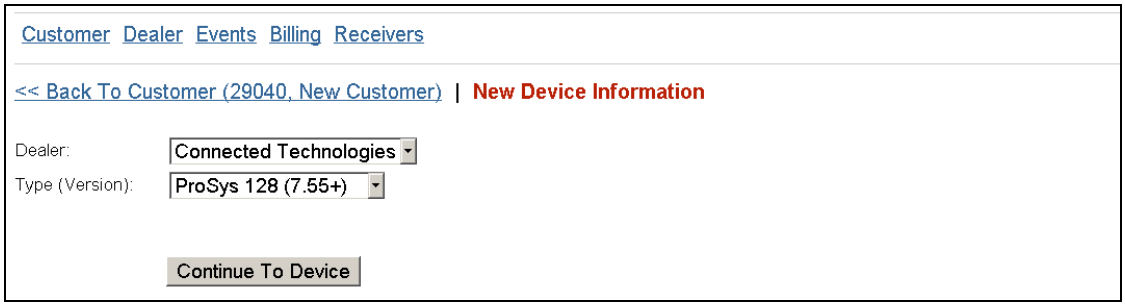
Setup Complete!

Create a Risco System


Customer Dealer Events Billing Receivers
<< Back To Customer (29040, New Customer) | New System Information
Name: Alarm Panel *
Site: Headquarters
Type: Risco Control Panel (ProSys 128,ProSys 16,ProSys 40...)
Continue

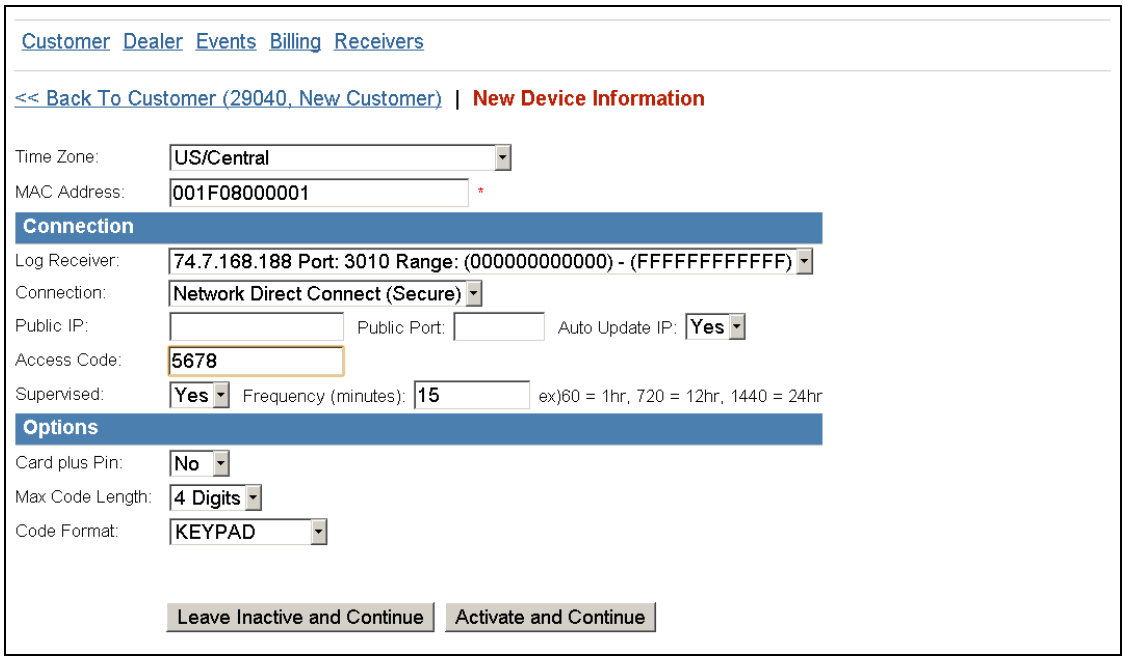
Create System Setup Form

1) Fill-in the required information about this system.
2) Choose the System Type from the drop-down.
3) Click “Continue”.


Customer Dealer Events Billing Receivers
<< Back To Customer (29040, New Customer) | New Device Information
Dealer: Connected Technologies
Type (Version): ProSys 128 (7.55+)
Continue To Device

Create Device Type Setup Form

4) Choose the Device Type and Version from the drop-down. If you are unsure of the version, the device will correct it upon it communicating any programming commands.
5) Click “Continue to Device”


Customer Dealer Events Billing Receivers
<< Back To Customer (29040, New Customer) | New Device Information
Time Zone: US/Central
MAC Address: 001F08000001 *
Connection
Log Receiver: 74.7.168.188 Port: 3010 Range: (000000000000) - (FFFFFFFFFFFF)
Connection: Network Direct Connect (Secure)
Public IP: Public Port: Auto Update IP: Yes
Access Code: 5678
Supervised: Yes Frequency (minutes): 15 ex)60 = 1hr, 720 = 12hr, 1440 = 24hr
Options
Card plus Pin: No
Max Code Length: 4 Digits
Code Format: KEYPAD
Leave Inactive and Continue
Activate and Continue

Create Device Setup Form

6) Fill-in the required information about this device.
   ll. Enter the MAC Address
   mm. Set Log Receiver - This is the receiver programmed in the panel under Communication.
   nn. Enter the Access Code
   oo. Choose the Connection Type
      i. Network Direct Connect – Direct Connection via Network (SSL)
   pp. Public IP Address, Port, and Auto Update: If the Auto Update IP setting is Yes the public IP address is automatically determined upon the first communication with the panel and updated on each new connection.
   qq. Supervise Test: Enter the number of minutes that a test signal should be received from the panel. Hint: Add a grace time of at least 15 minutes.
   rr. Card plus Pin: Yes (Show field to enter Pin), No (Hide Pin Field)
   ss. Max Code Length: Display warning if customer attempts to enter a code with a higher length.
   tt. Code Format: Display warning if customer attempts to enter a code with a higher number than is possible based on this bit length. This is the same number programmed into the keypads. Example: Standard 26-Bit cards and keyfobs (16 Bits).
7) To continue, you may choose to activate the account now, which will start the billing, or to leave inactive if you are setting up this account ahead of the installation, skip to step 11 if leaving inactive.

Activate Device Form

8) Choose the service level from the drop-down.
9) Enter any comments.
10) Click “Save”.

11) Program the Control Panel

ProSYS Communication Setup

Communication Dialer1:

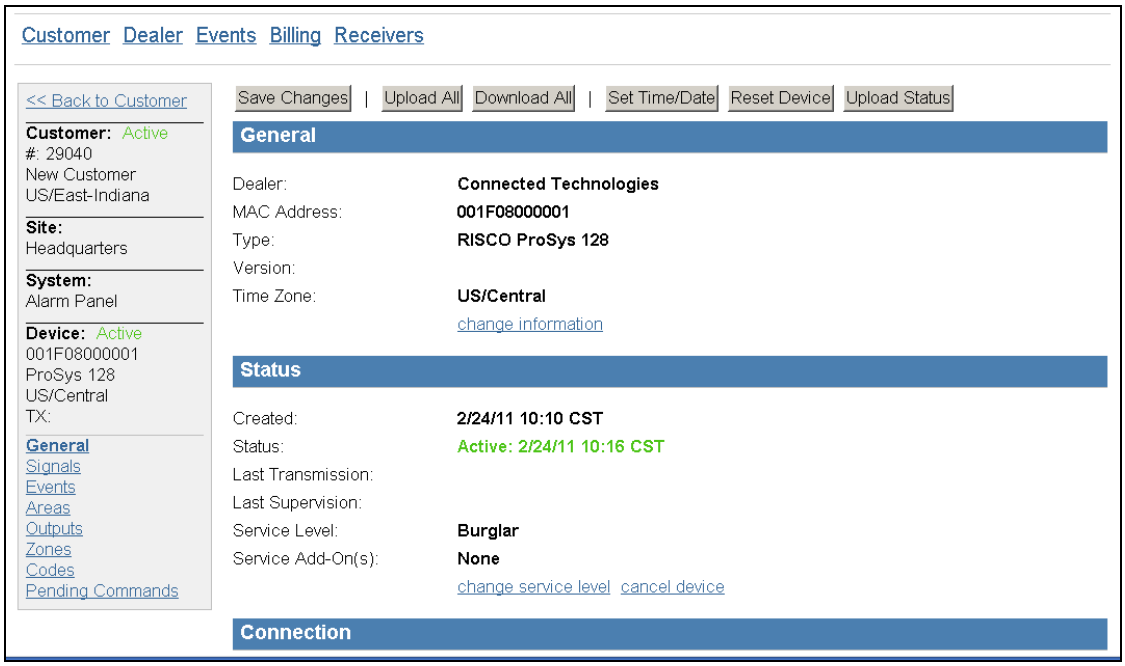
1) Choose MS ph1,ph2, or ph3.
   - If this account is being monitored by a central station, Use ph2 or ph3.
   - If this account is NOT being monitored, Use ph1
2) Comm Format: 0420 for ContactID, 0700 for SIA
3) Channel Type: External IP
4) IP Address: dealer assigned by Connected Technologies
5) Port: dealer assigned by Connected Technologies

Communication Dialer 2:

1) Report Split: Be sure to include the path for Connect ONE in all categories, (MS arm/disarm, MS urgent, & MS non urgent)

Communication ACM:

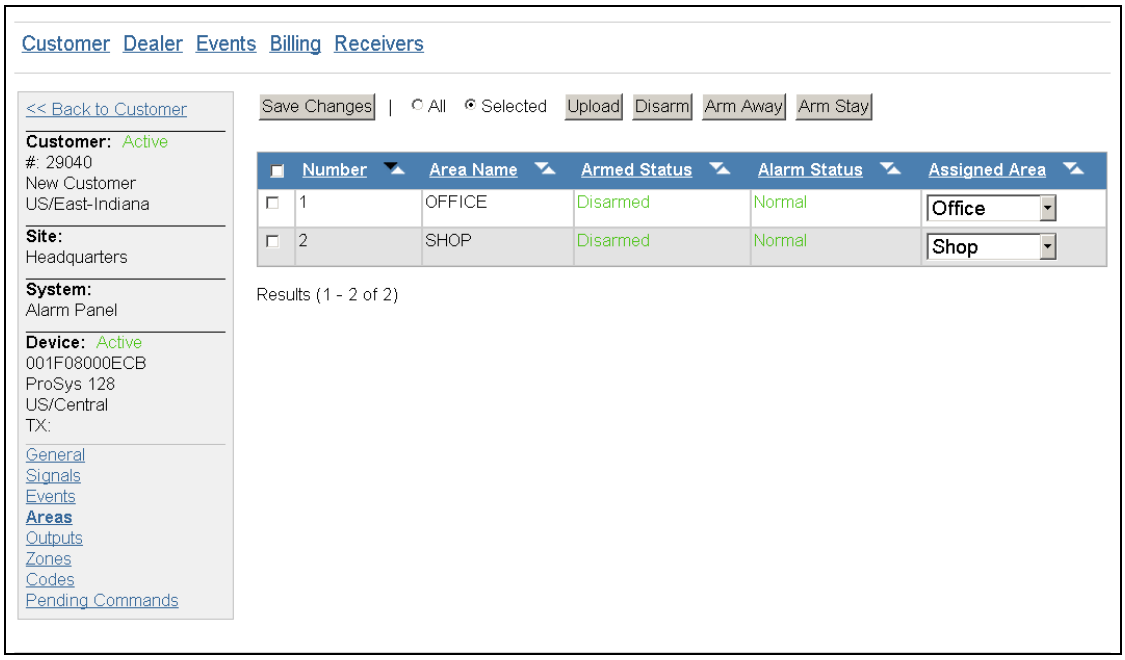
1) Client Authentication: Enable
2) MS Polling: Set to any frequency desired, ex) 360 = 1 hour



Device View

12) Click “Receive All”, this will enter the commands to receive all of the necessary information from the control panel. Once the commands have processed, continue through this guide.

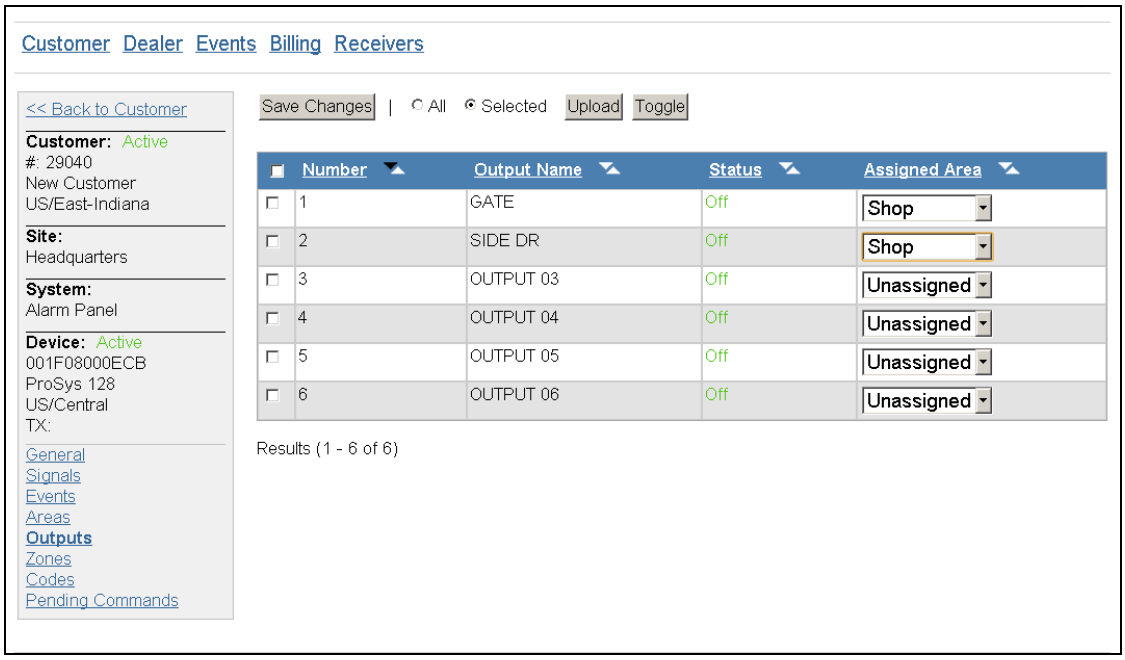
13)Click on “Areas”, the following screen should appear.



Device Areas

14) Assign each device area to a site area using the “Assigned Area” drop-down box.
15) Click “Save Changes”

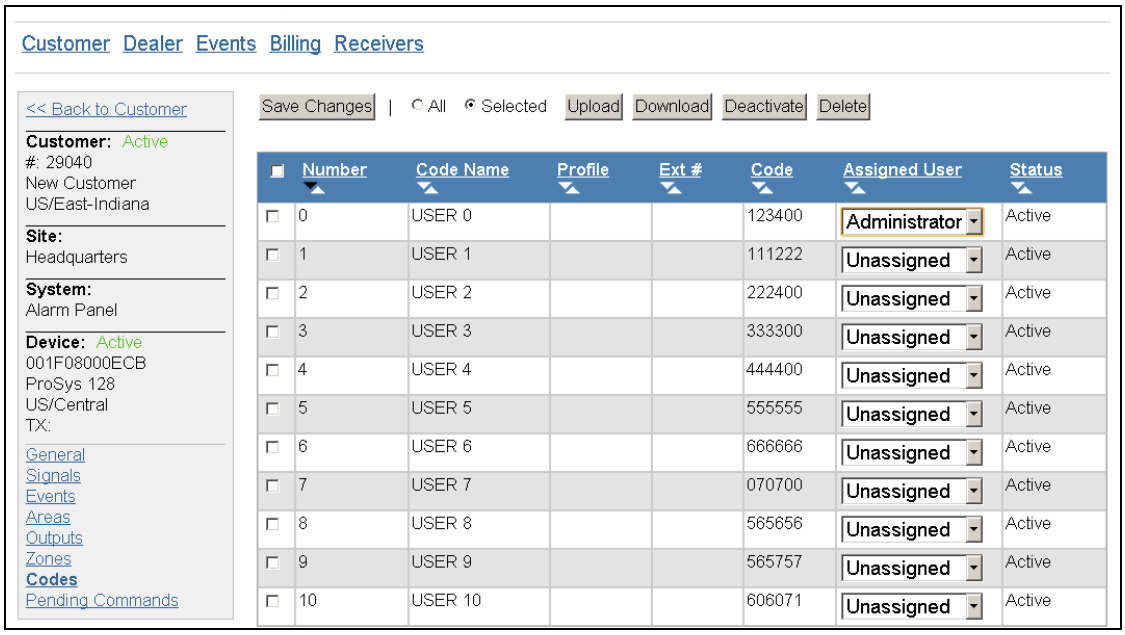
16) Click on “Outputs”, the following screen should appear. – IF APPLICABLE



Device Outputs

17) Assign each device output to a site area using the “Assigned Area” drop-down box. Only assign outputs that you want the customer to have control over. For instance, do not assign outputs that trip a radio.
18) Click “Save Changes”

19)Click on “Codes”, the following screen should appear.



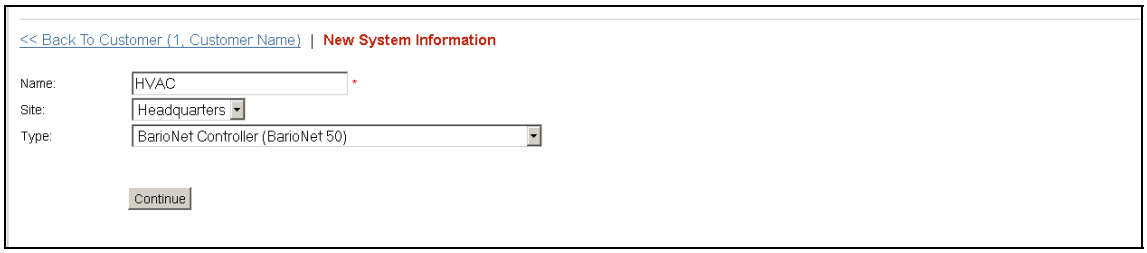
Device Codes

20) Assign the grand master level code to the Administrator user. This gives the system level permissions to the Administrator. These permissions are on the profile or authority level of the code you are assigning. For instance, arming/disarming, modify system codes, etc.

21) Click “Save Changes”

Setup Complete!

Create a Network Gateway System


<< Back To Customer (1, Customer Name) | New System Information
Name: HVAC *
Site: Headquarters
Type: BarioNet Controller (BarioNet 50)
Continue

Create System Setup Form

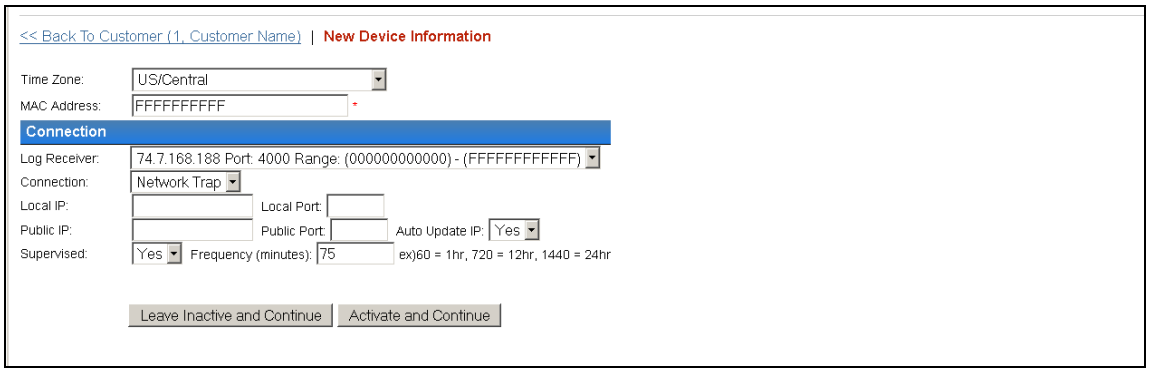
1) Fill-in the required information about this system.
2) Choose the System Type from the drop-down.
3) Click “Continue”.

<< Back To Customer (1, Customer Name) | New Device Information
Dealer: Connected Technologies
Type (Version): BarioNet 50 (1.00+)
Continue To Device

Create Device Type Setup Form

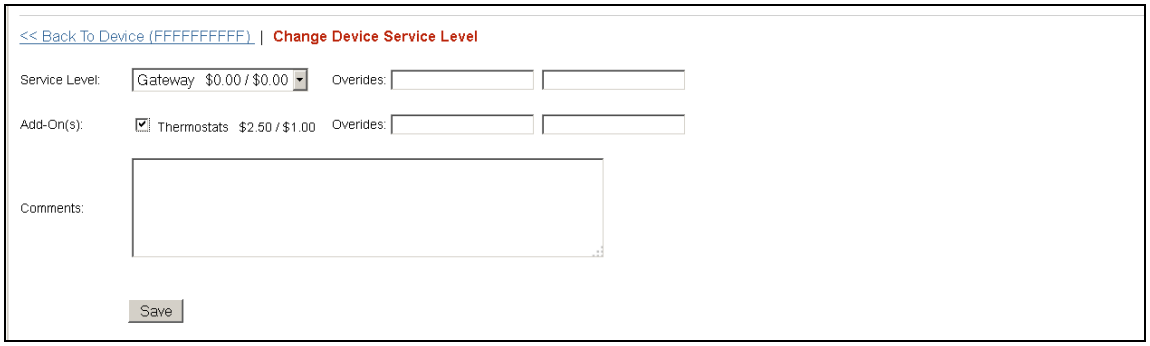
4) Choose the Device Type and Version from the drop-down. If you are unsure of the version, the device will correct it upon it communicating any programming commands.

Click “Continue to Device


<< Back To Customer (1, Customer Name) | New Device Information
Time Zone: US/Central
MAC Address: FFFFFFFFFF
Connection
Log Receiver: 74.7.168.188 Port: 4000 Range: (000000000000) - (FFFFFFFFFFFF)
Connection: Network Trap
Local IP: Local Port:
Public IP: Public Port: Auto Update IP: Yes
Supervised: Yes Frequency (minutes): 75 ex)60 = 1hr, 720 = 12hr, 1440 = 24hr
Leave Inactive and Continue
Activate and Continue

Create Device Setup Form

5) Fill-in the required information about this device.
   uu. Enter the MAC Address, No dashes.
   vv. Local IP Address & Port – This may be left blank for now and will be updated when using the "Receive All" button on the next screen.
   ww. Public IP Address, Port, and Auto Update: If the Auto Update IP setting is Yes the Public IP address is updated on each new connection.
   xx. Supervise Test: Enter the number of minutes that a test signal should be received from the thermostat. Hint: Add a grace time of at least 15 minutes.
6) To continue, you may choose to activate the account now, which will start the billing, or to leave inactive if you are setting up this account ahead of the installation, skip to step 10 if leaving inactive.


<< Back To Device (FFFFFFFFFF) | Change Device Service Level
Service Level: Gateway $0.00 / $0.00 Overides:
Add-On(s): Thermostats $2.50 / $1.00 Overides:
Comments:
Save

Activate Device Form

7) Choose the service level from the drop-down.
8) Enter any comments.
9) Click "Save".

10) Power-up the network gateway and all thermostats
11) The network gateway comes set to DHCP by default, so it should acquire an address on its own. If a DHCP server is unavailable at the site, a local static IP address will have to be programmed into the network gateway. To do so follow the steps below. Please note you can skip these steps if a DHCP server is available at the site and proceed to step 12.

Setting temporary IP address using ARP command
This procedure is to temporarily set the IP address for the first time browser access.
Attention:
After this procedure the temporary IP will be active only as long as the Barionet stays powered. After a restart the procedure has to be repeated unless you have configured the IP address as described in the next chapter.
Step 1
Use either a “crossover” network cable between the Barionet and the PC or use two network cables to connect the Barionet and the PC to a network switch.
Step 2
Make sure that you have a valid IP address configured on your PC (e.g. 192.168.0.2) and power the Barionet.
Step 3
Open a command window with a click on “Start” followed by a click on “Run..”.
In the “Open” field type **cmd** and click on “OK”
Step 4
Please skip this step if you used a “crossover” network cable in step 1 and proceed to step 5.
To ensure that we use a free IP address (not already used by another device in the network) we have to use the Ping command.
In this example we assume the PC to have the IP address “192.168.0.2” and want to check if “192.168.0.6” is free.
To do so type into the command window
ping 192.168.0.6 and hit the “Enter” key.
If you get a reply (IP already used) then try to ping another IP until you find one that is not used.
If the request times out (as shown in the above window) then the “pinged” IP is free and we can continue with the next step.
Step 5
Now we are going to make your PC talk to the

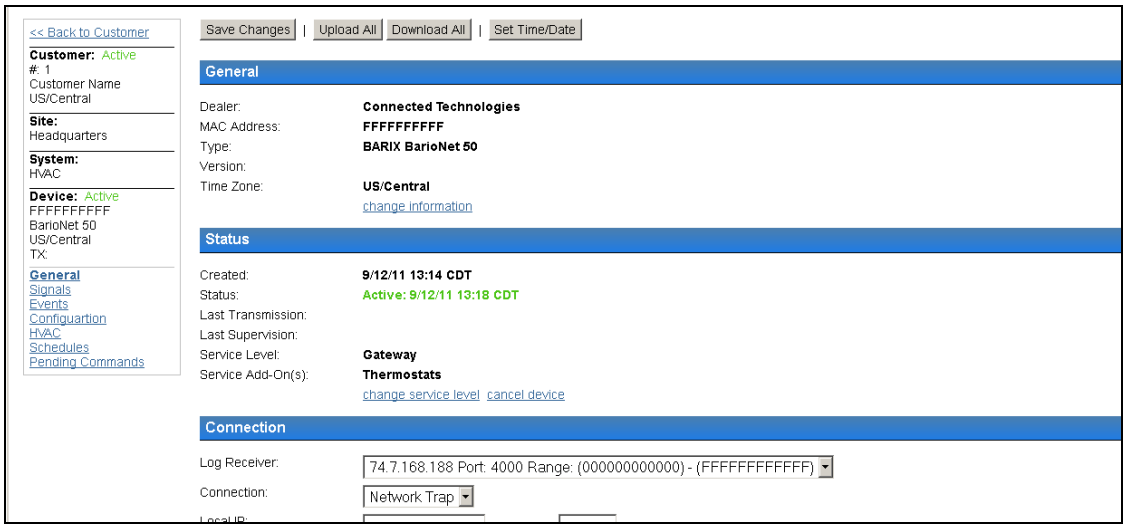
Barionet's MAC address using the IP address 192.168.0.6. (The MAC address of the Barionet unit is printed on a label placed on the bottom of the device) using the “arp” command with parameter “-s” for “set” followed by the chosen IP address and the MAC address (12 hex digits, separated by a hyphen every 2 digits)
To do so type into the command window
arp -s 192.168.0.6 00-20-4A-93-7F-D4
and hit the “Enter” key.

Step 6

Now we have to make the Barionet listening to the IP address 192.168.0.6 using the Telnet command.
To do so type into the command window
telnet 192.168.0.6 1
and hit the “Enter” key (the number “one” must be there for this command to work correctly !!!)
The Barionet will refuse the connection on port 1 (one) immediately but will be available for web access on the IP address used as long as the Barionet stays powered.

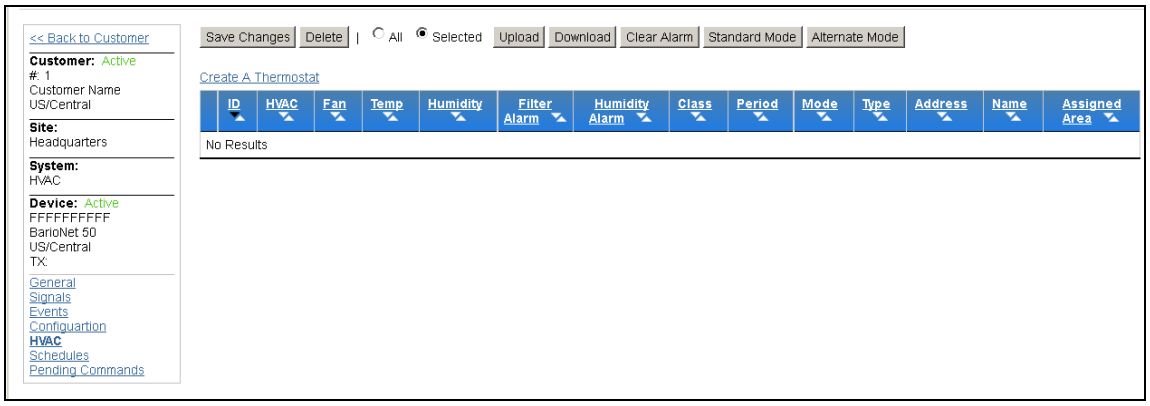
Step 7

To check if the Barionet is responding you can use the ping command again. To do so type into the command window
ping 192.168.0.6
and hit the “Enter” key.
If you do get a reply (as shown in the above window) the IP address 192.168.0.6 can be used to access the Barionet using a web browser. Please proceed to the next chapter to set the IP address permanently.
If you do get “Request timed out” instead of a reply then please repeat step 6 carefully (most likely mistyped the telnet command).



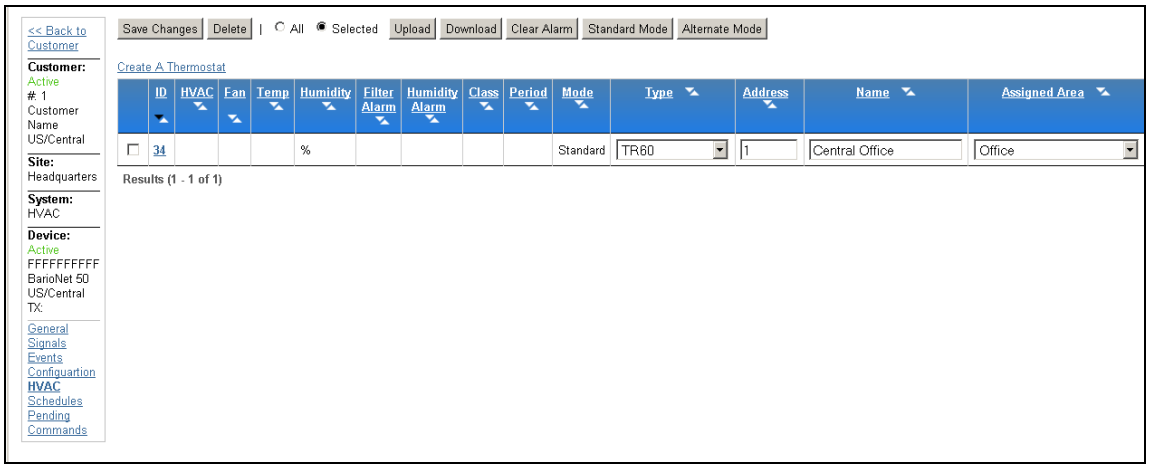
Device View

12)Click on “HVAC”, the following screen should appear.



Device HVAC

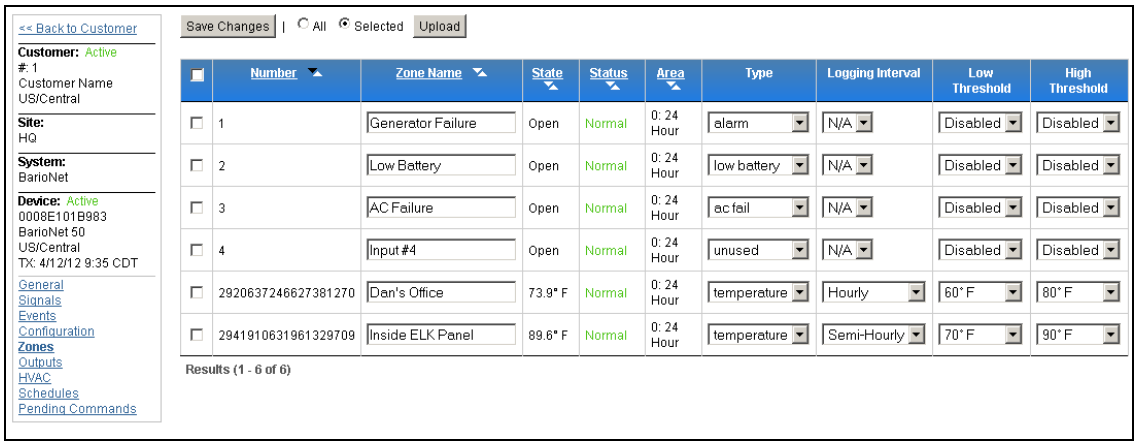
13)Click on “Create a Thermostat”, the following screen should appear.



Device HVAC

14) Assign the thermostat type, serial address, name, and the site area using the "Assigned Area" drop-down box. Note: the serial address must be set on each thermostat. Refer to the thermostat instructions for the setup mode to set this serial address.
15) Click "Save Changes"
16) Repeat steps 91 – 93 for each thermostat.
17) Click "General" from the left links, this will return you to the main device page.
18) Click "Receive All", this will enter the commands to receive all of the necessary information from the gateway. Wait for all commands to process prior to continuing.
19) Refer to the last page for a thermostat wiring schematic.

20) Click on Zones, the following screen will appear.


<< Back to Customer
Customer: Active
#: 1
Customer Name
US/Central
Site:
HQ
System:
BarioNet
Device: Active
0008E101B983
BarioNet 50
US/Central
TX: 4/12/12 9:35 CDT
General
Signals
Events
Configuration
Zones
Outputs
HVAC
Schedules
Pending Commands
Save Changes | All Selected Upload
Number | Zone Name | State | Status | Area | Type | Logging Interval | Low Threshold | High Threshold
1 | Generator Failure | Open | Normal | 0: 24 Hour | alarm | N/A | Disabled | Disabled
2 | Low Battery | Open | Normal | 0: 24 Hour | low battery | N/A | Disabled | Disabled
3 | AC Failure | Open | Normal | 0: 24 Hour | ac fail | N/A | Disabled | Disabled
4 | Input #4 | Open | Normal | 0: 24 Hour | unused | N/A | Disabled | Disabled
2920637246627381270 | Dan's Office | 73.9° F | Normal | 0: 24 Hour | temperature | Hourly | 60° F | 80° F
2941910631961329709 | Inside ELK Panel | 89.6° F | Normal | 0: 24 Hour | temperature | Semi-Hourly | 70° F | 90° F
Results (1 - 6 of 6)

21) You may set the name and type for the zones which appear. The first 4 zones are the dry contact input zones, the zones after are the 1-wire temperature sensors.

22) The dry contact input zones can be set to the following types:

yy. Unused

zz. Alarm / Restore, ex) Water Detection
   i. Generates Alarm and Restore Events

aaa. Trouble / Restore, ex) Generator Failure
   i. Generates Trouble and Restore Events

bbb. AC Fail Reporting, ex) Power Supply AC Failure
   i. Generates AC Fail and Restore Events

ccc. Low Battery Reporting, ex) Power Supply Low Battery
   i. Generates Low Battery and Restore Events

ddd. Fault (open / close messages), ex) Server Room Door
   i. Generates Open and Close Events

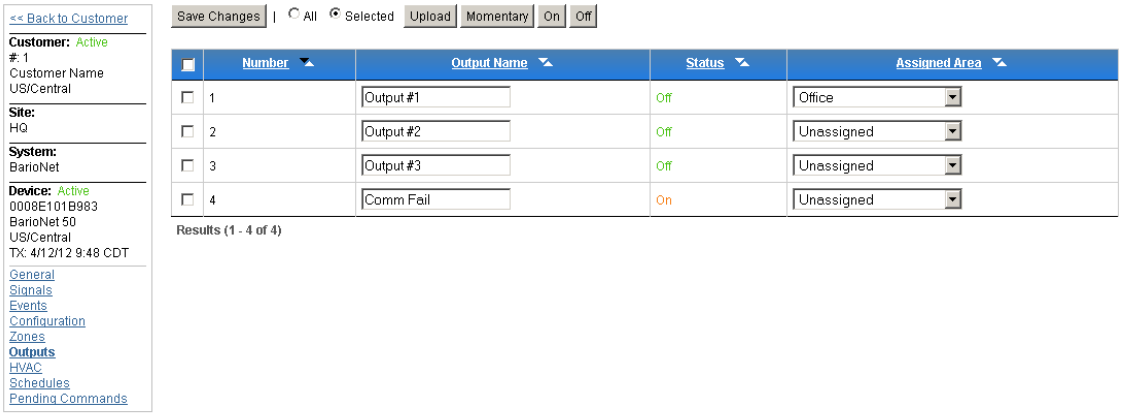
23) Temperature Sensors will automatically be set to the temperature type

eee. If subscribed temperature zones may be logged on the following intervals
   i. Semi-Hourly (every 30 minutes)
   ii. Hourly
   iii. Bi-Hourly (every 2 hours)

fff. Low and High threshold levels may be set which will generate low / high temperature alarm events when reached

24) Click Save Changes, after all settings are set.

25) Click on Outputs and the following screen will appear.



26) The 4 relay outputs may be named and assigned to an area. Once assigned your customer will be able to control the output.

ggg. Outputs 1-3 are general purpose outputs

hhh. Output 4 is a dedicated communication failure output

i. This relay follows the communication status of the network gateway and turns off when in failure. A failure condition will be detected after 15 minutes. Connect this output to a SPDT relay to drive a light and/or sounder when the relay is in the off position. This will produce a local alert of the failure so it can be corrected quickly.

ii. Your customer may also receive an email/text message of a failure if you configure an Interaction Rule to watch for communication event types and the device is set to be supervised, this option is set on the device general page.

27) Refer to the recommended wiring diagram on the next page

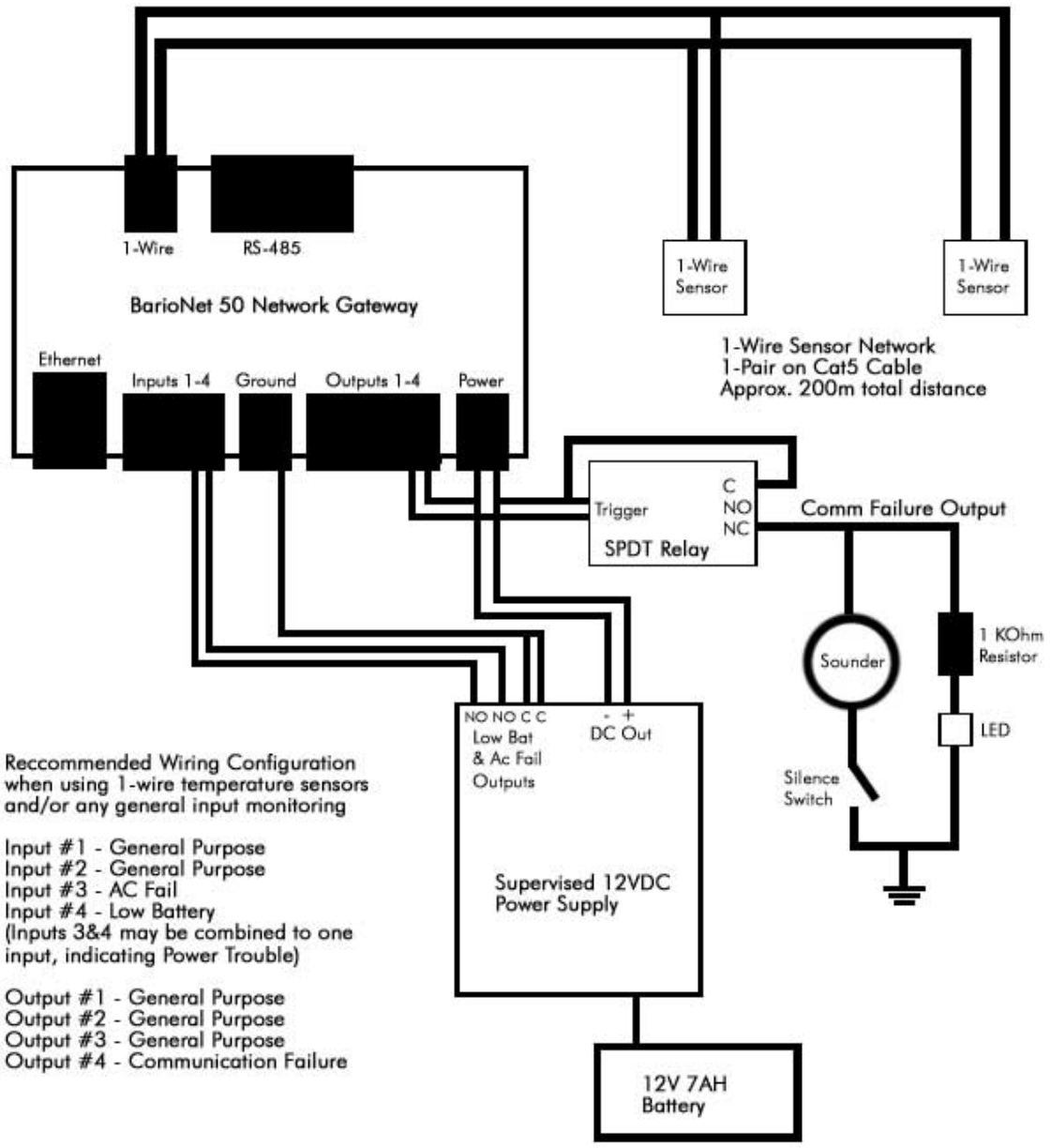
Setup Complete!

1-Wire Temperature Sensor Wiring Diagram (No Alarm Panel)

(No Alarm Control Panel)

Supervised 12/24VDC Power Supply - Connect the Low Battery and AC Fail outputs to inputs on the gateway for monitoring. Connect the communication failure, output 4, on the gateway to a local sounder plate. The plate may also have a led and silence switch.

I**MPORTANT NOTE** *(Long Wire Runs)*: Install a 2kOhm pull-up resistor at the Barionet 1W terminal to the Barionet +5V terminal.



Connected Technologies
A 6110 Lou Street Crystal Lake, IL 60014 | P 815.301.4280 F 815.301.4286 | www.connectedtechnologies.us

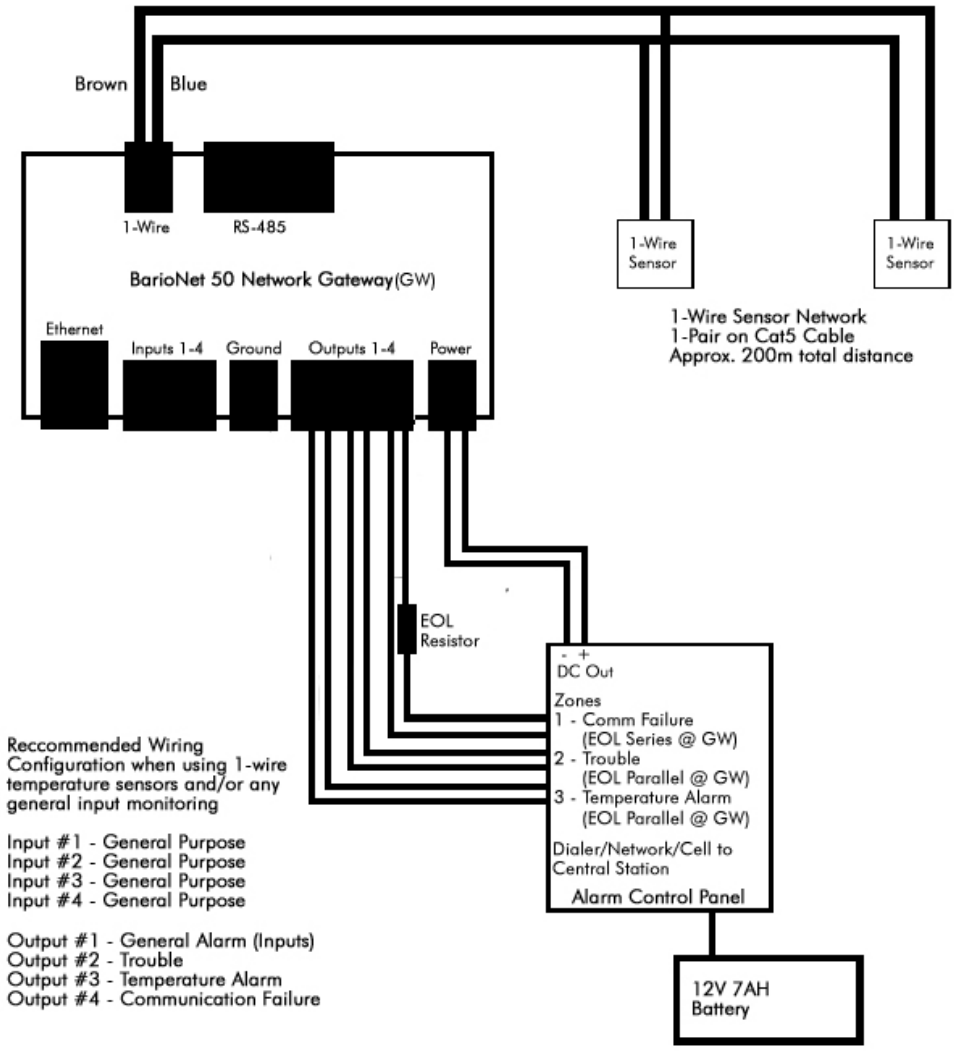
1-Wire Temperature Sensor Wiring Diagram (CS Alarm Hookup)

(Alarm Control Panel –Communications on Alarm Panel to Central Station)

NOTE: The Alarm/Trouble/Temperature Alarm Outputs on the Network Gateway will require a network connection to Connect ONE to operate when the condition exists. The Communication Failure output will work regardless of the network connection which will indicate the central station that an alarm could be missed because of the communication failure.

Connect output 4 on the gateway to a zone on the alarm control panel. Connect output 2 on the gateway to a zone on the alarm to indicate general trouble, and output 3 on the gateway to a zone on the alarm to indicate temperature alarm. Optionally connect output 1 on the gateway to a zone on the alarm to indicate general alarm, connect outputs on the alarm control panel to the inputs on the gateway and monitor for ac and low battery conditions. A keypad and sounder may be connected to the alarm control panel for local annunciation.

I**MPORTANT NOTE** *(Long Wire Runs)*: Install a 2kOhm pull-up resistor at the Barionet 1W terminal to the Barionet +5V terminal.



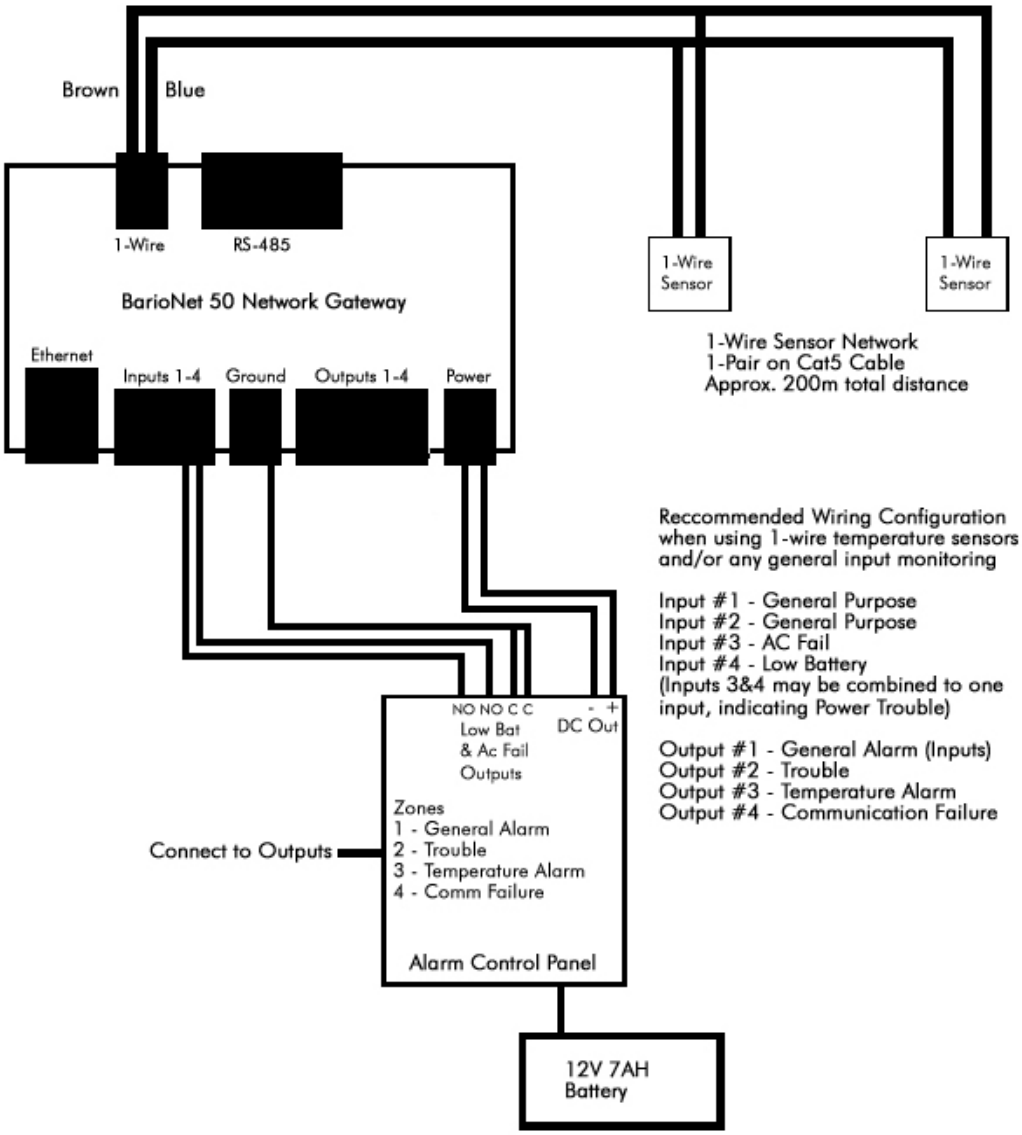
Connected Technologies
A 6110 Lou Street Crystal Lake, IL 60014 | P 815.301.4280 F 815.301.4286 | www.connectedtechnologies.us

1-Wire Temperature Sensor Wiring Diagram (Local Alarm Hookup)

(Alarm Control Panel – No Communications on Alarm Panel - LOCAL ONLY)

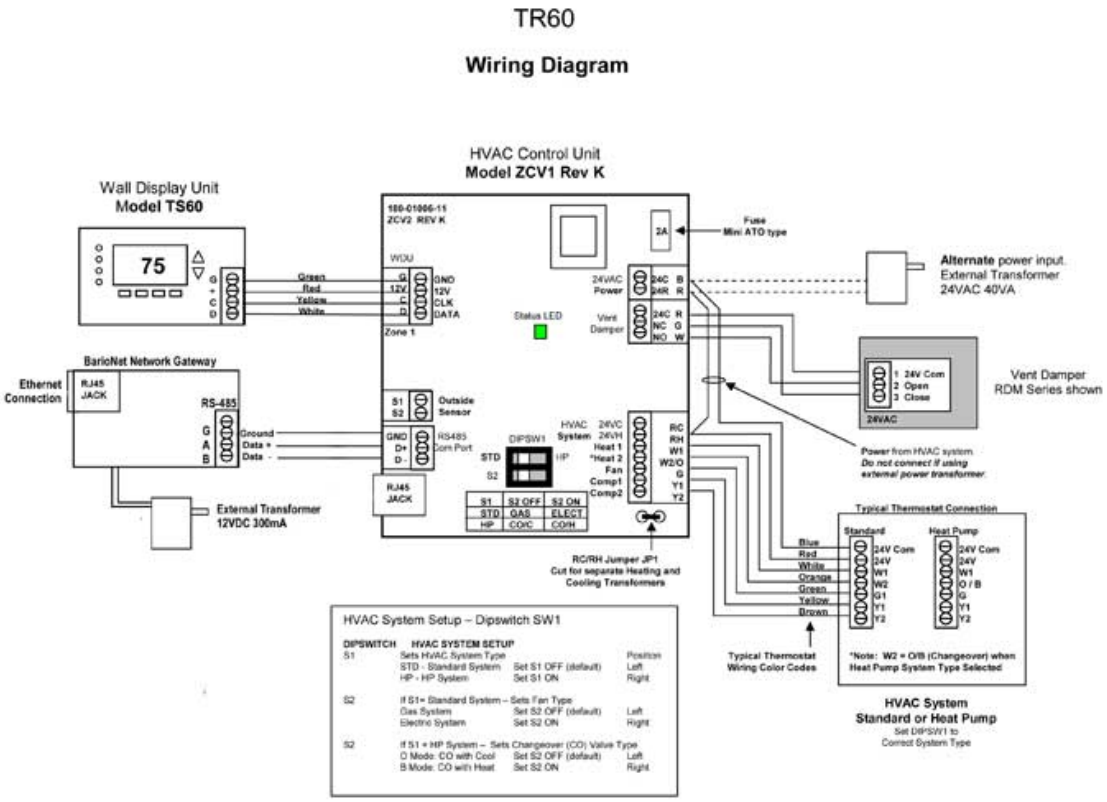
Connect outputs on the alarm control panel to the inputs on the gateway and monitor for ac and low battery conditions. Connect output 4 on the gateway to a zone on the alarm control panel. Optionally also connect output 1 on the gateway to a zone on the alarm to indicate general alarm, output 2 on the gateway to a zone on the alarm to indicate general trouble, and output 3 on the gateway to a zone on the alarm to indicate temperature alarm. A keypad and sounder may be connected to the alarm control panel for local annunciation. Note outputs 1, 2, and 3 will not change state unless the gateway has good communication to the receiver. Output 4 on the gateway will turn off if the connection is lost which will indicate the problem.

I**MPORTANT NOTE** *(Long Wire Runs)*: Install a 2kOhm pull-up resistor at the Barionet 1W terminal to the Barionet +5V terminal.



Connected Technologies
A 6110 Lou Street Crystal Lake, IL 60014 | P 815.301.4280 F 815.301.4286 | www.connectedtechnologies.us

RCS Thermostats Wiring Diagram

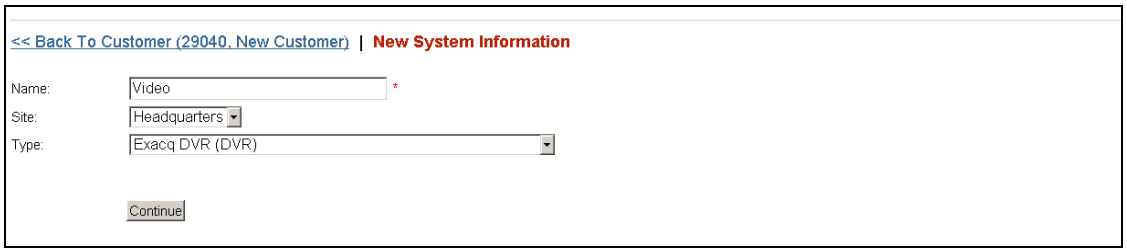


Notes:
Actual current draw of BarioNet gateway is 150mA max. It may be powered from another 12VDC source, such as the alarm panel, however it draws too much to be powered from the WDU terminals on the ZCV1 control board.

The BarioNet Network Gateway comes preconfigured for Connect ONE's servers and set to DHCP. As long as the end-user's network has a DHCP server, there is zero configuration of the gateway. If they do not have a DHCP server then the only configuration is to set the local IP address.

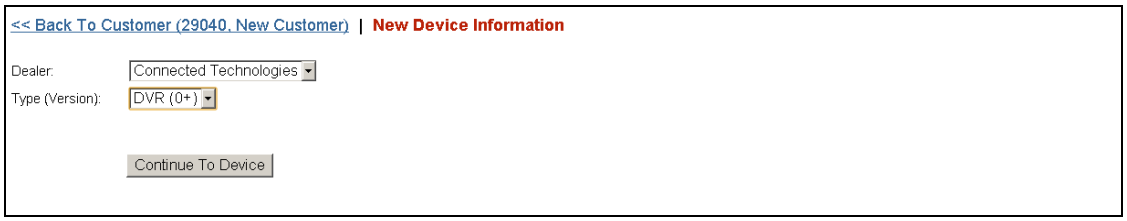
Application Example:
The HVAC controller (ZCV1) can be located either at the furnace/RTU or in the case of a drop-tile ceiling (such as many commercial buildings) the controller can be located above the drop-tile ceiling immediately above the thermostat location. This will eliminate the need to perform any installation at the RTU.

Create an Exacq / Ganz / Geovision System



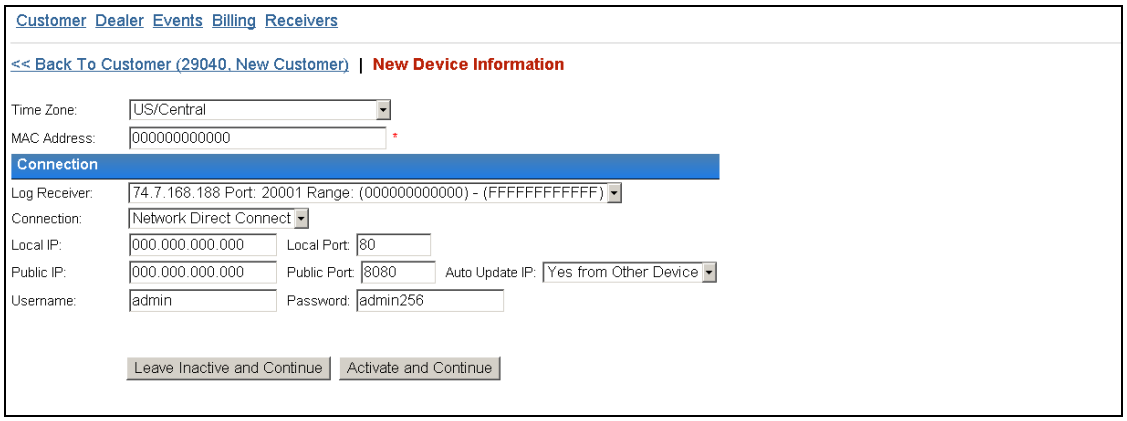
Create System Setup Form

1) Fill-in the required information about this system.
2) Choose the System Type from the drop-down.
3) Click “Continue”.


<< Back To Customer (29040, New Customer) | New Device Information
Dealer: Connected Technologies
Type (Version): DVR (0+)
Continue To Device

Create Device Type Setup Form

4) Choose the Device Type and Version from the drop-down. If you are unsure of the version, the device will correct it upon it communicating any programming commands.
5) Click “Continue to Device”


Customer Dealer Events Billing Receivers
<< Back To Customer (29040, New Customer) | New Device Information
Time Zone: US/Central
MAC Address: 000000000000 *
Connection
Log Receiver: 74.7.168.188 Port: 20001 Range: (000000000000) - (FFFFFFFFFFFF)
Connection: Network Direct Connect
Local IP: 000.000.000.000 Local Port: 80
Public IP: 000.000.000.000 Public Port: 8080 Auto Update IP: Yes from Other Device
Username: admin Password: admin256
Leave Inactive and Continue
Activate and Continue

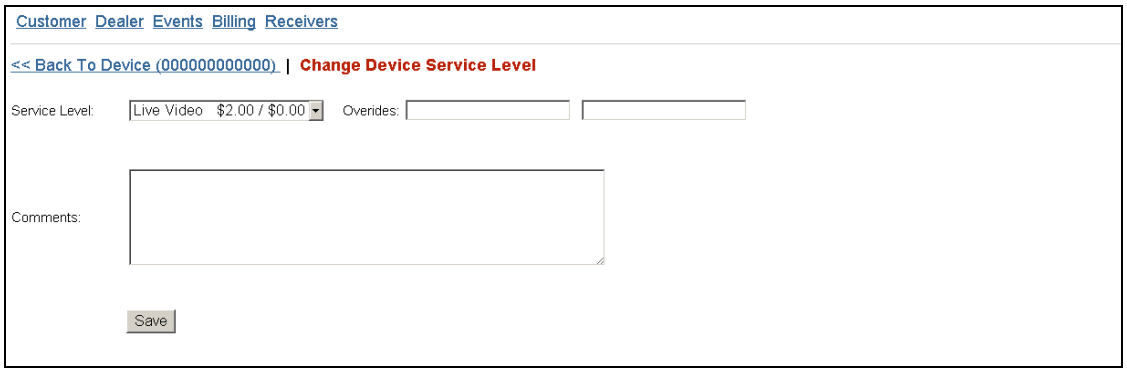
Create Device Setup Form

6) Fill-in the required information about this device.
   iii. Public IP Address, Port, and Auto Update: If the Auto Update IP setting is “Yes from Other Device” the public IP address is automatically determined upon the next communication from another device at this site, such as the burglar/access system. It will also automatically update on each new connection.
   jjj. Enter the Local IP Address and Port
   kkk. Enter the Username and Password

Ganz Systems Only: After receiving the camera names, the customer may lockdown their firewall to only allow connections from their own white listed IP addresses. No video ever passes through Connect ONE servers, the video is fed from a direct connection between the customer’s browser and their DVR device.

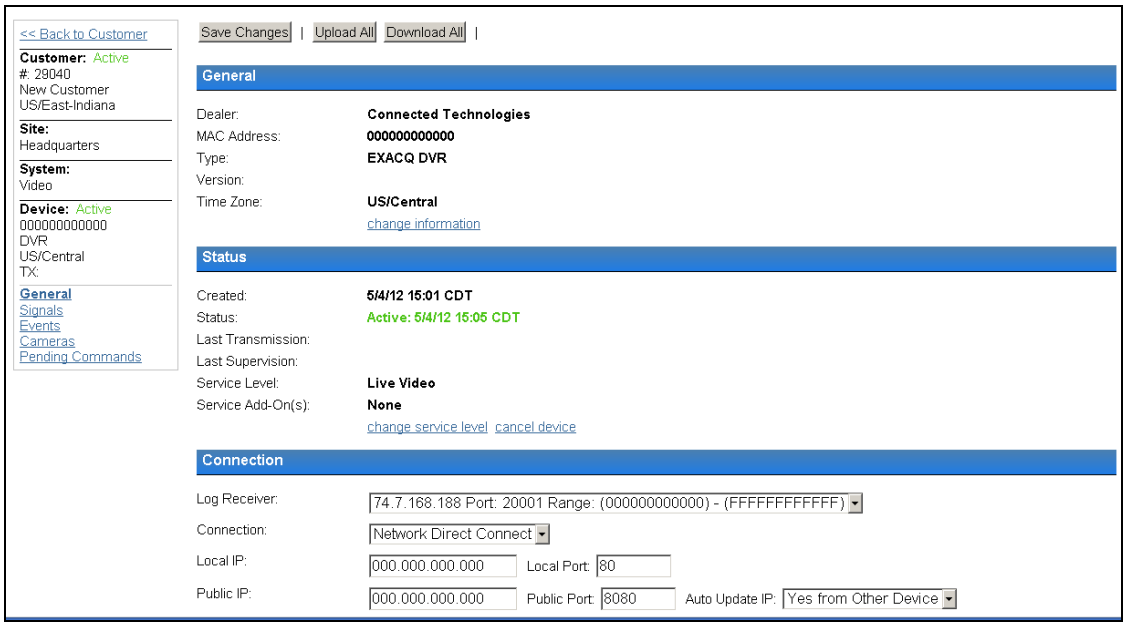
Exacq & Geovision Systems: Connect ONE servers must login prior to connecting the video from the DVR. This login procedure requires the customer allow Connect ONE servers access to the DVR. Currently the IP addresses are outbound.e0.connected.cc and outbound.w0.connected.cc. No video ever passes through Connect ONE servers, the video is fed from a direct connection between the customer’s browser and their DVR device.

7) To continue, you may choose to activate the account now, which will start the billing, or to leave inactive if you are setting up this account ahead of the installation, skip to step 11 if leaving inactive.



Activate Device Form

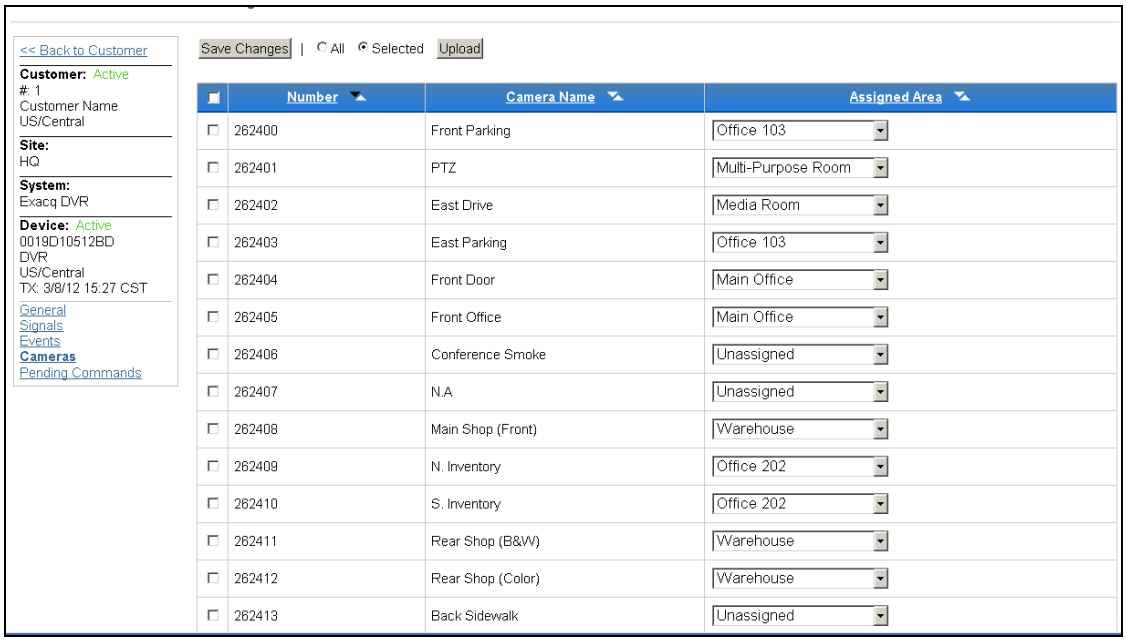
8) Choose the service level from the drop-down.
9) Enter any comments.
10) Click “Save”.



Device View

11) Click “Receive All”, this will enter the commands to receive all of the necessary information from the DVR. Once the commands have processed, continue through this guide.

12)Click on “Cameras”, the following screen should appear.

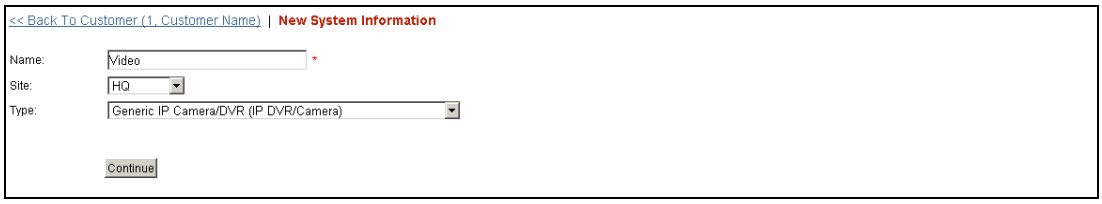


Device Cameras

13) Assign each camera to a site area using the “Assigned Area” drop-down box.
14) Click “Save Changes”

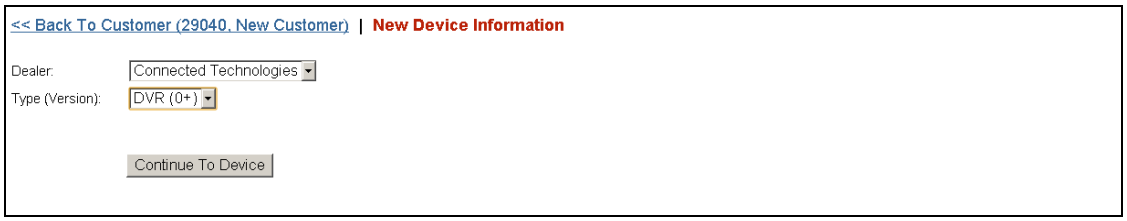
Setup Complete!

Create a Generic IP Camera/DVR System



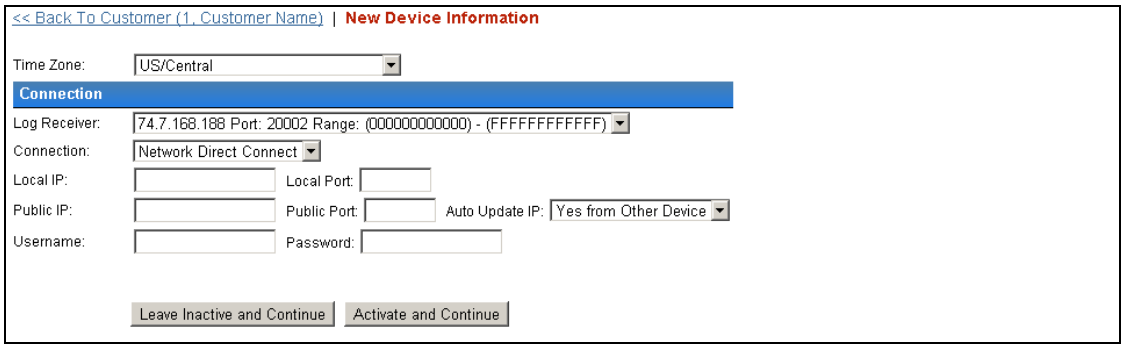
Create System Setup Form

1) Fill-in the required information about this system.
2) Choose the System Type from the drop-down.
3) Click “Continue”.



Create Device Type Setup Form

4) Click “Continue to Device”

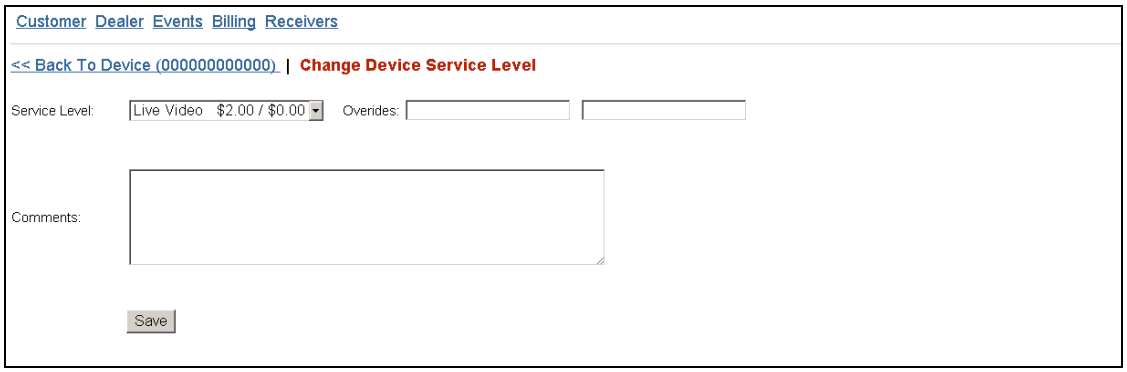

<< Back To Customer (1, Customer Name) | New Device Information
Time Zone: US/Central
Connection
Log Receiver: 74.7.168.188 Port: 20002 Range: (000000000000) - (FFFFFFFFFFFF)
Connection: Network Direct Connect
Local IP: Local Port:
Public IP: Public Port: Auto Update IP: Yes from Other Device
Username: Password:
Leave Inactive and Continue
Activate and Continue

Create Device Setup Form

5) Fill-in the required information about this device.
   lll. Public IP Address, Port, and Auto Update: If the Auto Update IP setting is "Yes from Other Device" the public IP address is automatically determined upon the next communication from another device at this site, such as the burglar/access system. It will also automatically update on each new connection.
   mmm. Enter the Local IP Address and Port
   nnn. Enter the Username and Password (If Required)

Note: The customer may lockdown their firewall to only allow connections from their own white listed IP addresses. No video ever passes through Connect ONE servers, the video is fed from a direct connection between the customer's browser and their video device.

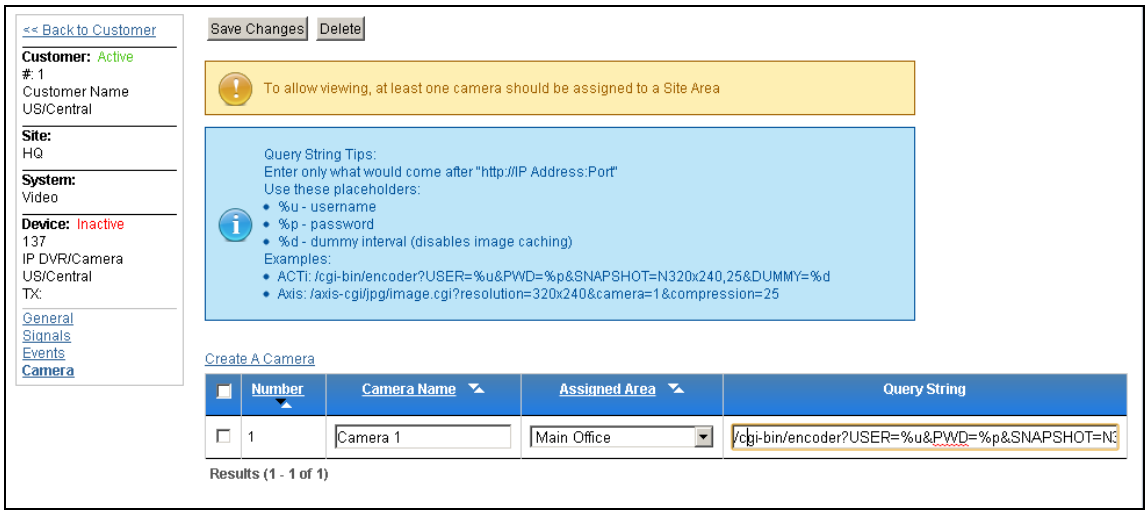
6) To continue, you may choose to activate the account now, which will start the billing, or to leave inactive if you are setting up this account ahead of the installation, skip to step 10 if leaving inactive.


Customer Dealer Events Billing Receivers
<< Back To Device (000000000000) | Change Device Service Level
Service Level: Live Video $2.00 / $0.00 Overides:
Comments:
Save

Activate Device Form

7) Choose the service level from the drop-down.
8) Enter any comments.
9) Click "Save".

10)Click on “Cameras”, the following screen should appear.



Device Cameras

11) Click on “Create A Camera”, A new camera record will be added
12) Enter the desired name, assign the camera to a site area using the “Assigned Area” drop-down box, and enter the query string.
    a. Be sure to only enter what would follow after the IP address into the query string field.
    b. If your camera is not listed, refer to the user manual of the camera for how to retrieve a snapshot or jpeg image via a url
    c. Multiple cameras can be added if the device is a multi-channel encoder or there are different ways of retrieving multiple images of the same camera.
13) Click “Save Changes”

Setup Complete!

Live Video - IT Instructions

1) Add or assign a user on the DVR for Connect ONE Live Viewing Access of all Cameras

2) Configure Router for Port Forwarding public port (# of their choosing) to local IP address of DVR on port 80

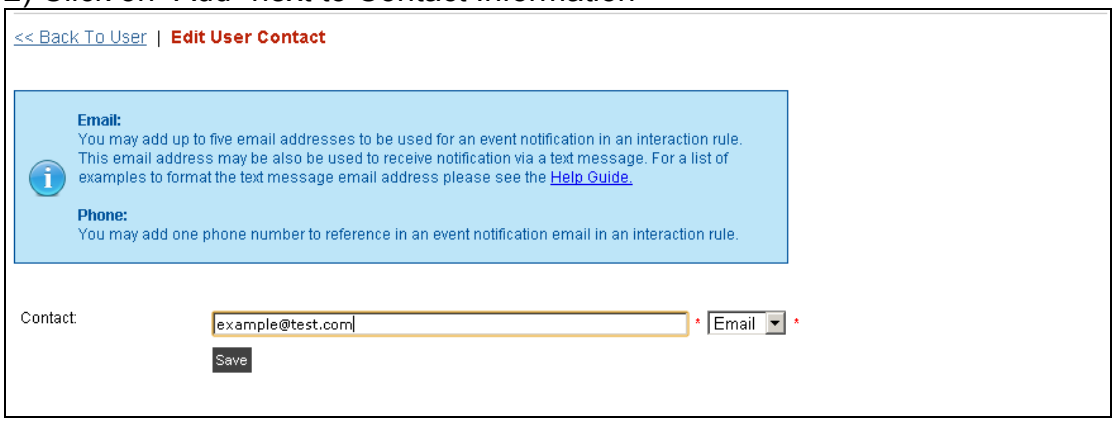
3) Configure Firewall to pass tcp traffic on port (# of their choosing) to local IP address of DVR on port 80

4) Notify dealer of public IP address, public port, local IP address, username and password

How to Setup an Action Rule for Notifications

1) Enter User Email / Text Messaging Addresses, click on Users then click on the user to edit

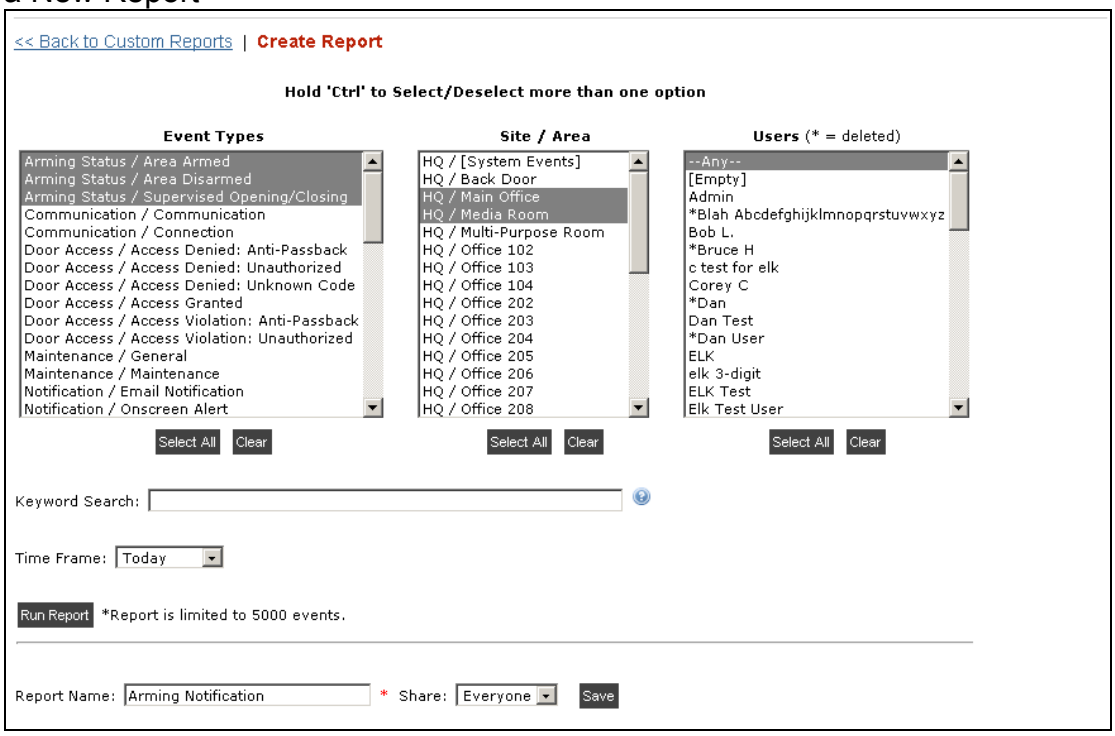
2) Click on “Add” next to Contact Information


<< Back To User | Edit User Contact
Email:
You may add up to five email addresses to be used for an event notification in an interaction rule. This email address may be also be used to receive notification via a text message. For a list of examples to format the text message email address please see the Help Guide.
Phone:
You may add one phone number to reference in an event notification email in an interaction rule.
Contact:
example@test.com
Email
Save

3) Enter a email address or text messaging address, click Save

Repeat steps 2 and 3 for each address for this user

4) Create a Filter Report – click on Reporting, then Custom Reports, then Create a New Report



5) Select the Event Type(s), Site Area(s), and User(s) to filter, and optional Keyword Filter
6) Enter a Name for the report and click Save

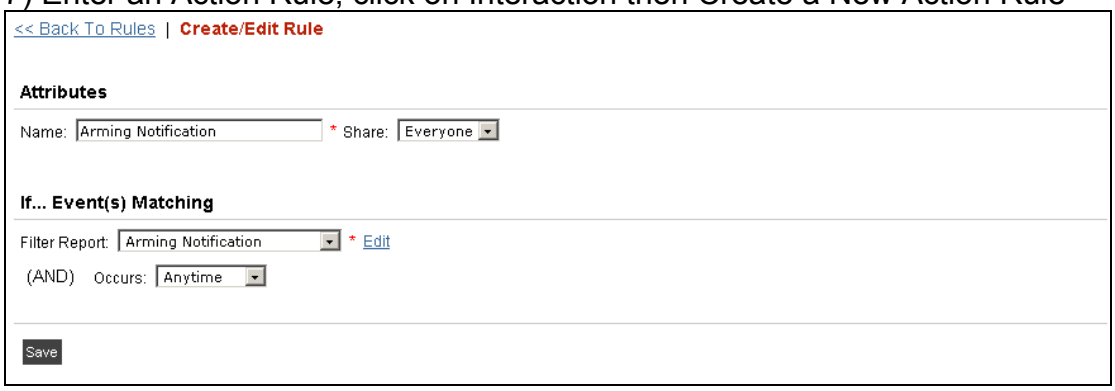
Hint:
This screenshot shows how to setup a filter for arming, disarming, and supervised open/close events, that are limited to the main office and media room areas only.

Use the “Site / [System Events]” area selection for event types such as AC Power, Communication Troubles, etc., that are not related to a specific area. For these types of events choose the “Any” user option as these will not be related to a particular user.

When filtering by user, be certain that the event will be generated by that user. For instance do not choose a user when filtering for alarm events, as the control panel can not know who generated the alarm, so use the “Any” user option.

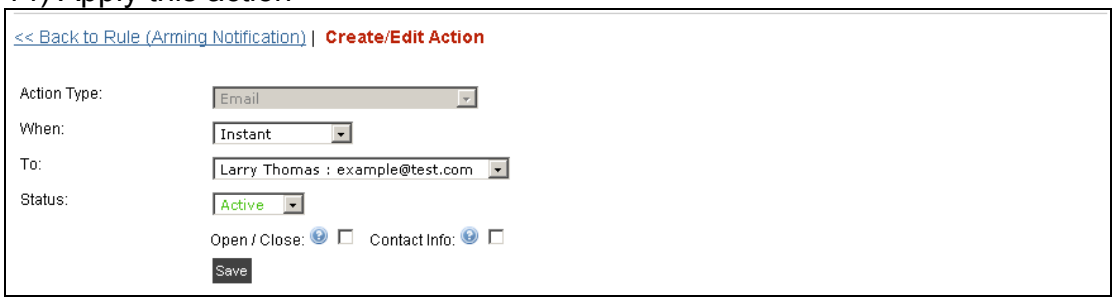
The keyword option can be used to filter by door name, zone name, etc. For example, to only filter alarms on the front door zone, choose the event type alarm and enter a keyword of Front Door, exactly how it is listed in the zone name.

7) Enter an Action Rule, click on Interaction then Create a New Action Rule



8) Enter an appropriate Name
9) Select the Filter Report you created in step 4.
10) You may choose to limit this action by a schedule. For instance if you only want to receive the notification outside of normal business hours choose the "Not During" timeframe and enter 8:00 to 17:00 Mon-Fri. This will only notify you if the event occurs outside of these times and not during the normal hours.
11) Click Save
12) Add an Action

13) Choose Email for email and text messages, click Continue
14) Apply this action



15) Select "When" to receive the notification, Instant, or in a Daily or Weekly Report. If Daily or Weekly the notification will occur at midnight and include all of the events that occurred in a report form.
16) Click Save

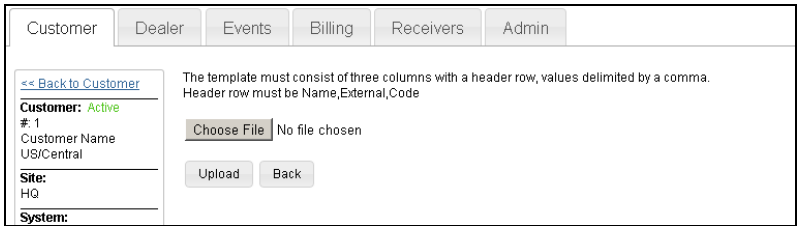
Code Import Utility

Create a csv file, easiest way is from excel. Start with a three column sheet, there must be a header row and it must be labeled (name, external, code) for each respective column. Once each row is filled in with the codes to import, then save the file and choose the type as “CVS (Comma delimited) (*.csv)”. The external field is optional and is not required to be populated but must be present.

Example Listing:

Name	External	Code
Bob Smith	234234	2312
Fred Jones	5678	341243
April Johnson	3456	4324

Now go to the dealer site, find the customer and device. Click on codes, then the Import button on the top of the list. From here you will upload the csv file, then click Upload.



A new page will load showing all the codes to be added/changed. From here you select which profile you would like for each code and whether to assign it to an existing user or create a new user from the code.